Part No. NN47250-101 (320665-G)
October 2007

4655 Great America Parkway
Santa Clara, CA 95054

Nortel WLAN Management Software 2300 Series User Guide

NORTEL

Copyright © 2007 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks and Service Marks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Legal Information

This section includes the following legal information:

- "Trademarks and Service Marks" on page 2
- "Limited Product Warranty" on page 3

Limited Product Warranty

The following sections describe the Nortel standard Product Warranty for End Users.

Products

WLAN—Security Switch 2300 Series

WLAN—Access Points (2330/2330A/2330B and series 2332)

Limited Warranty

Nortel standard warranty for hardware is one (1) year. Nortel warrants software materials to be defect free for 90 Days from time of purchase. Nortel requires purchasing the software subscription if a customer would like to receive new WLAN—Security Switch (2300), Nortel WLAN — Management System software. This limited warranty extends only to you the original purchaser of the Product.

Exclusive Remedy

Your sole remedy under the limited warranty described above is, at Nortel's sole option and expense, the repair or replacement of the non-conforming Product or refund of the purchase price of the non-conforming Products. Nortel's obligation under this limited warranty is subject to compliance with Nortel's then-current Return Material Authorization ("RMA") procedures. All replaced Products will become the property of Nortel. Exchange Products not returned to Nortel will be invoiced at full Product list prices. Replacement Products may be new, reconditioned or contain refurbished materials. In connection with any warranty services hereunder, Nortel may in its sole discretion modify the Product at no cost to you to improve its reliability or performance.

Warranty Claim Procedures

Should a Product fail to conform to the limited warranty during the applicable warranty period as described above, Nortel must be notified during the applicable warranty period in order to have any obligation under the limited warranty.

The End Customer or their designated reseller must obtain a Return Material Authorization number (RMA number) from Nortel for the non-conforming Product and the non-conforming Product must be returned to Nortel according to the then-current RMA procedures. The End Customer or their designated reseller is responsible to ensure that the shipments are insured, with the transportation charges prepaid and that the RMA number is clearly marked on the outside of the package. Nortel will not accept collect shipments or those returned without an RMA number clearly visible on the outside of the package.

Exclusions and Restrictions

Nortel shall not be responsible for any software, firmware, information or memory data contained in, stored on or integrated with any Product returned to Nortel pursuant to any warranty or repair.

Upon return of repaired or replaced Products by Nortel, the warranty with respect to such Products will continue for the remaining unexpired warranty or sixty (60) days, whichever is longer. Nortel may provide out-of-warranty repair for the Products at its then-prevailing repair rates.

The limited warranty for the Product does not apply if, in the judgment of Nortel, the Product fails due to damage from shipment, handling, storage, accident, abuse or misuse, or it has been used or maintained in a manner not conforming to Product manual instructions, has been modified in any way, or has had any Serial Number removed or defaced. Repair by anyone other than Nortel or an approved agent will void this warranty.

EXCEPT FOR ANY EXPRESS LIMITED WARRANTIES FROM Nortel Networks SET FORTH ABOVE, THE PRODUCT IS PROVIDED “AS IS”, AND Nortel Networks AND ITS SUPPLIERS MAKE NO WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO PRODUCT OR ANY PART THEREOF, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THOSE ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. Nortel Networks’S SUPPLIERS MAKE NO DIRECT WARRANTY OF ANY KIND TO END CUSTOMER FOR THE LICENSED MATERIALS. NEITHER Nortel Networks NOR ANY OF ITS SUPPLIERS WARRANT THAT THE LICENSED MATERIALS OR ANY PART THEREOF WILL MEET END CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, OR ERROR-FREE, OR THAT ANY ERRORS IN THE PRODUCT WILL BE CORRECTED. SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO END CUSTOMER. THIS LIMITED WARRANTY GIVES END CUSTOMER SPECIFIC LEGAL RIGHTS. END CUSTOMER MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE/JURISDICTION TO STATE/JURISDICTION.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL Nortel Networks OR ITS SUPPLIERS BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF PROFITS, OR FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES (OR DIRECT DAMAGES IN THE CASE OF Nortel Networks’S SUPPLIERS) ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE ARISING OUT OF OR RELATED TO THE PRODUCT OR ANY USE OR INABILITY TO USE THE PRODUCT. Nortel Networks’S TOTAL LIABILITY ARISING OUT OF OR RELATED TO THE PRODUCT, OR USE OR INABILITY TO USE THE PRODUCT, WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THE LIMITATIONS SET FORTH IN THIS SECTION SHALL APPLY EVEN IF Nortel Networks AND/OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. Nortel Networks NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Disclaimer

This network plan was generated by the WMS planning tool using a predictive RF model. This information is an estimate of the amount, configuration, and placement of WLAN 2300 equipment and is intended to facilitate project cost projections.

A Wireless LAN site survey service captures actual RF data to accurately model RF environments and is the best method to determine correct location of APs, and therefore installation locations of cabling. A WMS network plan is an approximation only and does not substitute for a Wireless LAN site survey.

Contents

Contents 7

How to get help 13

Introducing the Nortel WLAN 2300 Series System 15
Nortel WLAN 2300 System 15
Documentation 16
Safety and Advisory Notices 17
Text and Syntax Conventions 17

Getting Started 19
Hardware Requirements for WLAN Management Software Client 19
Hardware Requirements for WMS Services 20
Software Requirements 20
Preparing for Installation 21
User Privileges 21
Serial Number and License Key 21
HP OpenView Network Node Manager 22
Resource Allocation 22
WMS Services Options 23
Installing WLAN Management Software 23
Unpacking Files 24
Using the Installation Wizard 24
Start WMS Services 25
Connect WMS Clients to WMS Services 26
Configure WMS Services 26
WLAN Management Software Access Control 29
WLAN Management Software Interface 30
Displaying the Main Window 30
Using the Toolbar and Menu Bar 31
Setting Preferences 31
Easy Configuration Using Wizards 32
Getting Help 32

Planning and Managing Your Wireless Network with WMS. 35
Which Services to Provide? 35
Network Plan 36
RF Coverage Area 36
Auto-RF 37
Auto-RF with Modelling 37
RF Planning 37
Which Planning Method Should I Use? 38
Configuration 39
Wireless Configuration 40
AAA Security Configuration 42
Authentication 42
Authorization 45
Accounting 45
System and Administration Configuration 45
Configure Basic WSS Properties 46
Configure WSS Connection Information 46
Configure Boot Information 46
Equipment Installation 46
Deployment 47
Management and Monitoring 47
Network Status 48
RF Monitoring 48
Client Monitoring 48
Fault Management 49
Rogue Detection 49
Verification 49
RF Plan Optimization 51

Configuring Wireless Services 53
What Are Services? 53
Configure Employee Access Services 54
Task Table 54
Step Summary 56
Example: Configure Employee Access 56

Create a Radio Profile 57
Configure RADIUS Servers 58
Create a Service Profile for 802.1X Access 62
View the Service Profile's Access Rules 65
Set Up VLANs on WSSs 66
What's Next? 69
Configure Guest Access Services 69
Task Table 70
Step Summary 72
Create a User Group and Guest Users 73
Create a Service Profile for Guest Access with Web Login 76
View the Service Profile's Access Rules 84
Optional: Configure Mobility Profiles 84
What's Next? 85
Configure Voice over Wireless IP Service 85
Task Table 86
Step Summary 87
Create a Radio Profile for Voice 88
Create a Service Profile for Voice 89
Create a Service Profile for WMM VoWIP Devices 89
Create a Service Profile for SVP VoWIP Devices 93
Create a Service Profile for Avaya VoWIP Devices 95
Create a Service Profile for Vocera VoWIP Devices 98
Set Up a VLAN for VoWIP on WSSs 99
What's Next? 100

Using Auto-RF 101
What Is Auto-RF? 101
Place the Equipment 102
Configure Initial WSS Connectivity 102
Upload the WSS Configuration into a WMS Network Plan 102
Create a Service Profile 103
Create a Radio Profile and Map the Service Profile to It 104
Create Your APs 104
Apply a Radio Profile to Each Radio 107
What's Next? 108

Using Auto-RF with Modelling 109
What Is Auto-RF with Modelling? 109
Add Site Information 109
Insert RF Obstacles 113
Create Your RF Coverage Area 115
Create a Wiring Closet 115
Create Your RF Coverage Area 116
Add APs 124
Associate APs to the Coverage Area 124
What's Next? 127

Using RF Planning 129
What Is RF Planning? 129
Prepare the Floor Drawings 130
Define Site Information 131
Import a Floor Plan 136
Set the Scale 137
Clean Layout 138
Model RF Obstacles 140
Import a Site Survey 142
Plan RF Coverage 142
Add Wiring Closets 143
Create Coverage Areas 144
Compute and Place APs 151
Assign Channel Settings 154
Calculate Optimal Power 155
Display Coverage 156
Generate a Work Order 157
Install the Equipment 158
What's Next? 159

Managing and Monitoring Your Network 161
What Is Network Management? 161
What Is Network Monitoring? 161
Deploy Your Configuration 162
Perform Basic Administrative Tasks 163

Configuring WSS Management Services 163
Distribute System Images 164
Using the Image Repository 164
Distributing System Images 165
Saving Versions of Network Plans 166
Import and Export Switch Configuration Files 167
Monitoring Examples 168
Monitor an Individual User 169
Find the User 170
Locate the User 173
Display User Activity 175
View User Performance Statistics 177
Monitor a Group of Users 179
What's Next? 182

Managing Alarms 183
What Is Fault Management? 183
Set Up the Fault Management System 183
Classify and Organize Faults 185
Search Capabilities 185
Manage Faults 186
Alarm Summary 186
Alarm Summary Details 187
Top 5 Sources of Alarms 187
Intrusion Detection System (IDS) Alarms 188
Denial of Service (DoS) Alarms 188
Store Faults and Retrieve Fault History 189
Generate Alarm Reports 190
Alarm Summary Report 190
Alarm History Report 191
Security and Client OUI Reports 192
Use the Fault Management System to Locate a Rogue 192
Configuring Countermeasures 196
What's Next? 200

Optimizing a Network Plan 201

Using RF Measurements from APs 201
Using RF Measurements from an Ekahau Site Survey 202
Generating an Ekahau Site Survey Work Order 203
Importing RF Measurements from the Ekahau Site Survey 206
Optimizing the RF Coverage Model 208
Locating and Fixing Coverage Holes 209
Displaying the RF Coverage Area 210
Locking Down APs 210
Fixing a Coverage Hole 210
Computing and Placing New APs 211
Replanning Your Network 211
What's Next? 211

Index 213

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel solutions center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting help from a specialist by using an express routing code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Introducing the Nortel WLAN 2300 Series System

Nortel WLAN 2300 System 15
Documentation 16

This guide provides information about planning, configuring, deploying, and managing a Nortel WLAN 2300 System wireless LAN (WLAN) using the WMS tool suite.

Read this guide if you are a network administrator or a person responsible for managing a WLAN.

Nortel WLAN 2300 System

The Nortel WLAN 2300 System is an enterprise-class WLAN solution that seamlessly integrates with an existing wired enterprise network. The Nortel system provides secure connectivity to both wireless and wired users in large environments such as office buildings, hospitals, and university campuses and in small environments such as branch offices.

The Nortel WLAN 2300 System fulfills the three fundamental requirements of an enterprise WLAN as follows:

1. It eliminates the distinction between wired and wireless networks.
2. It allows users to work safely from anywhere (*secure mobility*).
3. It provides a comprehensive suite of intuitive tools for planning and managing the network before and after deployment, greatly easing the operational burden on IT resources.

The Nortel WLAN 2300 System consists of the following components:

- **WLAN Management Software tool suite**—A full-featured graphical user interface (GUI) application used to plan, configure, deploy, and manage a WLAN and its users
- **One or more WLAN—Security Switches (WSSs)** —Distributed, intelligent machines for managing user connectivity, connecting and powering Access Point**s** (APs), and connecting the WLAN to the wired network backbone
- **Multiple Access Points (APs)** —Wireless access points (APs) that transmit and receive radio frequency (RF) signals to and from wireless users and connect them to a WSS
- **WLAN 2300 System Software (WSS Software)**—The operating system that runs all WSSs and APs in a WLAN. **WSS Software** is accessible through a command-line interface (CLI), the Web View interface, or the WLAN Management Software GUI

Documentation

Consult the following documents to plan, install, configure, and manage a Nortel WLAN 2300 System.

Planning, Configuration, and Deployment

- *Nortel WLAN Management Software 2300 Series User Guide* (this document). Instructions for planning, configuring, deploying, and managing the entire WLAN with the WLAN Management Software tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy Nortel equipment to provide those services, and how to optimize and manage your WLAN.
- *Nortel WLAN Management Software 2300 Series Reference Guide*. Detailed instructions and information for all WLAN Management Software planning, configuration, and management features.

Installation

- *Nortel WLAN—Security Switch 2300 Series Installation and Basic Configuration Guide*. Instructions and specifications for installing a WSS
- *Nortel WLAN—Security Switch 2300 Series Quick Start Guide*. Instructions for performing basic setup of secure (802.1X) and guest (Web-based AAA) access, and for configuring a Mobility Domain for roaming
- *Nortel WLAN—Access Point 2330/2330A/2330B Installation Guide*. Instructions and specifications for installing an AP and connecting it to a WSS
- *Nortel WLAN—Series 2332 Access Point Installation Guide*. Instructions and specifications for installing a Series 2332 AP and connecting it to a WSS

Configuration and Management

- *Nortel WLAN Management Software 2300 Series Reference Guide*. Instructions for planning, configuring, deploying, and managing the entire WLAN with the WLAN Management Software tool suite
- *Nortel WLAN 2300 System Software Configuration Guide*. Instructions for configuring and managing the system through the WSS Software CLI
- *Nortel WLAN 2300 System Software Command Line Reference*. Functional and alphabetic reference to all WSS Software commands supported on WSSs and APs

Safety and Advisory Notices

The following kinds of safety and advisory notices appear in this manual.

Caution! This situation or condition can lead to data loss or damage to the product or other property.

Note. This information is of special interest.

Text and Syntax Conventions

Nortel manuals use the following text and syntax conventions:

Convention	Use
Monospace text	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
Italic text	Designates command variables that you replace with appropriate values or highlights publication titles or words requiring special emphasis.
Menu Name > Command	Indicates a menu item. For example, **File > Exit** indicates that you select **Exit** from the File menu.
[ ] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
| (vertical bar)	Separates mutually exclusive options in command syntax.

Getting Started

Hardware Requirements for WLAN Management Software Client 19
Hardware Requirements for WMS Services 20
Preparing for Installation 21
Installing WLAN Management Software 23
WLAN Management Software Interface 30

This chapter contains information about recommended system requirements for optimum WMS performance, information about installing WMS client and WMS Services software, and an introduction to using the WMS interface.

Hardware Requirements for WLAN Management Software Client

Table 1 shows the minimum and recommended requirements to run the WMS client on Windows and Linux platforms.

Table 1: Hardware Requirements for Running WLAN Management Software Client on Windows and Linux Systems

	Minimum	Recommended
Processor	Intel Pentium 4, 2 GHz or equivalent	Intel Pentium 4, 3 GHz or equivalent
RAM	512 MB	1 GB
Hard drive space available	100 MB	200 MB
Monitor resolution	1024x768 pixels, 24-bit color	1600x1200 pixels, 32-bit color
CD-ROM drive	CD-ROM or equivalent	CD-ROM

Hardware Requirements for WMS Services

Table 2 shows the minimum and recommended requirements to run the WMS Services on Windows and Linux platforms.

Table 2: Hardware Requirements for Running WMS Services on Windows and Linux Systems

	Minimum	Recommended
Processor	Intel Pentium 4 2.4 GHz or equivalent	Intel Pentium 4 3.6 GHz or equivalent
RAM	1 GB	2 GB
Hard drive space available	1 GB	2 GB
Monitor resolution	1024x768 pixels, 24-bit color	1600x1200 pixels, 32-bit color
CD-ROM drive	CD-ROM or equivalent	CD-ROM

Software Requirements

WMS Client and WMS Services are each supported on the following operating systems:

- Microsoft Windows Server 2003, Microsoft Windows XP with Service Pack 1 or higher, or Microsoft Windows 2000 with Service Pack 4
- SUSE Linux 9.1 and Red Hat WS 3

Note. You must use the English version of the operating system you select. Operating system versions in other languages are not supported with WMS.

The following additional software is required for certain WMS features:

- Web browser (for example, Microsoft Internet Explorer 5.*x* or 6.*x* or Netscape Navigator 6.*x* or 7.*x*)—For displaying WMS online help, work orders, and reports
- Adobe Acrobat Reader 5.x or later (or plug-in)—For reading the manuals and release notes
- HP OpenView Network Node Manager 6.4 or later—Must be installed prior to WMS if you plan to use WMS in your HP OpenView environment

Preparing for Installation

Before installing WMS, make sure you have the appropriate administrative privileges on the system, a serial number, and a license key, if required. If you plan to install the HP OpenView plug-in for WLAN Management Software, which allows you to integrate WMS into an HP OpenView environment, make sure that HP OpenView is already installed.

User Privileges

Before installing WMS, make sure that you are logged in as a user who has permission to install software or logged in as an administrator.

If you are installing on the Linux platforms, you must log on with root privileges.

After you install WLAN Management Software, you can configure WLAN Management Software access privileges for the user accounts on the machine. Likewise, you can configure access privileges for the monitoring service, if installed. Access privileges for the WLAN Management Software client are completely independent of access privileges for the monitoring service and are configured separately.

Serial Number and License Key

The serial number is included with your WMS software packaging, on the box and also on the CD case.

You can use the serial number and a valid host name to request license keys for the following types of licenses:

- RF Planning—Enables the RF modelling features of planning. With an RF Planning license, you can create RF obstacles, compute and place equipment, assign radio channels, and optimize radio power settings. Without an RF Planning license, you still can import or create floor plans and create coverage areas.

Note. The RF Planning software does not support outdoor installations. Results obtained do not compensate nor account for obstacles and characteristics typically associated with outdoor environments. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.

- WLAN Management Software Services—Enables you to install WLAN Management Software Services (the WLAN Management Software server).

When requesting a license key, you must provide your serial number and the hostname of the system on which WMS is to be installed. You must also indicate the feature(s) for which you want to have a license. Specify the host name of the host where the client (for RF Planning) or server (for WMS Services) will be installed. The host name you provide when you request the key must match the host name on the host where you install the product.

Depending on the license, you might also have restrictions on the number of APs you can manage using WMS.

Nortel recommends that you request a license key through Nortel after installation. If that is not possible, contact the Nortel Enterprise Technical Support (NETS). (Refer to "How to get help" on page 13.)

HP OpenView Network Node Manager

If you want to integrate Nortel into your HP OpenView environment, you have the option of installing the HP OpenView plug-in required to use Network Node Manager with Nortel products. Make sure that HP OpenView is already installed before installing WMS with the plug-in.

Resource Allocation

Table 3 contains general recommended guidelines for hardware requirements and memory allocation based on the number of radios and WSSs your server will support. A larger number of WSSs suggests more connections and data processing, which requires more CPU power. A larger number of radios suggests more data (including client sessions), which requires more RAM and storage.

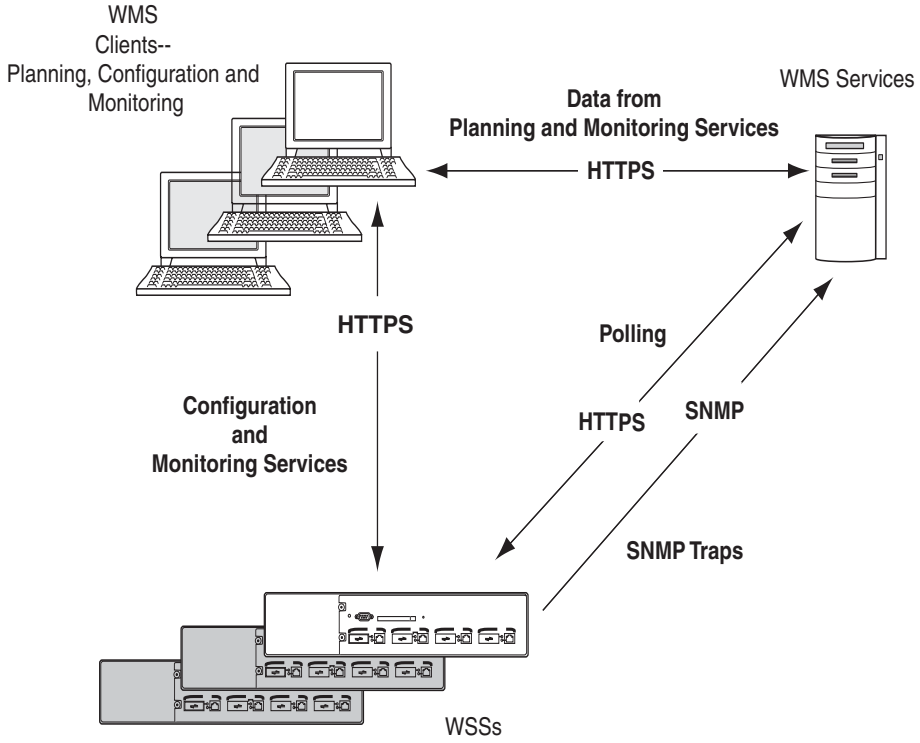
Table 3: Recommended Server Hardware Allocation

Number of Radios	1-25 WSSs	25-50 WSSs	50+ WSSs
1 – 1000	- 2.4 GHz P4 - 500 MB RAM - 1 GB HD	- 2.8 GHz P4 - 500 MB RAM - 1 GB HD	- 3.2 GHz Xeon - 1 GB RAM - 1 GB HD
1000 – 2000	- 2.4 GHz P4 - 1000 MB RAM - 2 GB HD	- 3.0 GHz P4 - 1000 MB RAM - 2 GB HD	- 3.6 GHz Xeon - 2 GB RAM - 2 GB HD

WMS Services Options

WMS Services can be installed either in standalone mode or shared mode. Standalone mode is when WMS client and WMS Services are installed on one machine. Standalone mode is primarily used for trying out WMS, while shared mode is used in a working environment. In shared mode, the administrator sets up WMS Services on a single host (typically with more resources) and other hosts with the client WMS application share WMS Services to access network plans and monitoring information. See Figure 1.

Figure 1: WLAN Management Software Services in Shared Mode



Installing WLAN Management Software

The same WMS install program installs either WMS client, WMS Services, or both.

This section contains information about the following topics:

- "Unpacking Files" on page 24
- "Using the Installation Wizard" on page 24

Unpacking Files

To unpack files on Windows systems

1. Insert the WMS CD in the CD-ROM drive. If Autorun is enabled, wait briefly for the install program to start. For more information about using the installation wizard, refer to "Using the Installation Wizard" on page 24.

   If Autorun is disabled, follow these steps:

   a. In Windows Explorer, navigate to your CD-ROM drive.

   b. In the Windows\VM directory, double-click **install.exe**.

   The Introduction page of the WMS installation wizard appears.

2. Click **Next** to display the Choose Installation Type page of the installation wizard and go to "Using the Installation Wizard" on page 24.

To unpack files on Linux systems

1. Log in as superuser.
2. Insert the WMS CD in the CD-ROM drive.
3. For the platform on which you are installing WMS, click the appropriate **Installer** link.
4. Save the installation binary to a directory.
5. Open a shell window.
6. Use the **cd** command to go to the directory in which you saved the installation binary.
7. In the shell window, type **sh./install.bin**. The Introduction page of the WMS installation wizard appears.
8. Click **Next** to display the Choose Installation Type page of the installation wizard and go to "Using the Installation Wizard" on page 24.

The installer does not make any path changes during installation. You might want to configure path information, to make WLAN Management Software easy to start on your system. WLAN Management Software must be run at the root level.

Using the Installation Wizard

To use the installation wizard

1. On the Choose Installation Type page, choose one of the following:
   - **To install both the WMS server and the client, click the WMS Services icon.**
   - **To install only the WMS client, click the WMS client icon.**

Note. For detailed installation instructions, refer to "Installing WMS" in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

Near the end of the installation process, the installer displays the following service ports that WLAN Management Software Services will use:

- 443—HTTPS server port
- 162—SNMP trap receiver port

You can change one or both port numbers to prevent conflicts with other applications on the same host.

Note. Multiple applications cannot use the same UDP or TCP port on the same host. For example, port 443 is defined by the Internet Assigned Numbers Authority (IANA) as the well-known HTTPS port. If the host on which you install WMS Services uses its default HTTPS port (443) and the same host also runs Microsoft Internet Information Services (IIS) on its default HTTPS port (443), there will be a conflict over the port. WLAN Management Software clients will not be able to communicate with WMS Services.

Note. If you plan to use the remote configuration option to configure new switches, you must use port 443 for WMS Services. When a switch requests its configuration from WMS Services, it sends the request to port 443.

Start WMS Services

The method for starting monitoring service depends on the platform on which the service is installed:

- Windows systems—WMS Services are started automatically when you complete installation and starts automatically whenever you restart your system.

To start the WMS Services on a Linux System

- Linux systems—You can start and stop the WMS Services manually from the command line using a shell script that is installed when you install WMS Services. You also can configure the WMS Services to start and stop automatically.

To configure WMS Services as a daemon on SUSE 9.1

The recommended way to add services to a SUSE 9.1 installation is with the **insserv** command. Enter commands such as the following (as root):

```
suse# cd /etc/init.d
suse# ln -s /opt/wms/bin/wms-services wms-services
suse# insserv wms-services
```

To configure WMS Services as a daemon on Red Hat WS 3

The recommended way to add services to a Red Hat WS 3 system is with the **chkconfig** command. Enter commands such as the following (as root):

redhat# cd /etc/init.d
redhat# **ln -s /opt/wms/bin/wms-services wms-services**
redhat# **chkconfig --add wms-services**

Connect WMS Clients to WMS Services

To connect the client to Services

1. Start WMS Services by doing one of the following:
   - **Select Start > Programs > Nortel > WMS > WMS.**
   - **On Linux systems, change directories to *WMS_installation_directory*/bin, and enter./wms.**

   The WMS Services Connection wizard is displayed.
2. Enter the IP address or fully-qualified hostname of the machine on which the service is installed.

   If WLAN Management Software Services is installed on the same machine as the one you are using to run WLAN Management Software client, enter 127.0.0.1 as the IP address. This is a standard IP loopback address.
3. Specify the service port, if different from the port number in the Service Port listbox.

Note. The port number used by the monitoring service must not be used by another application on the machine where the monitoring service is installed. If the port number is used by another application, change the port number on the monitoring service. (refer to "Configure WMS Services".)

4. Click **Next** to connect to the server.
5. If the Certificate Check dialog is displayed, click **Accept**.

If you left the Open Network Plan option on the WLAN Management Software Services Connection dialog selected, the server opens a new (blank) network plan.

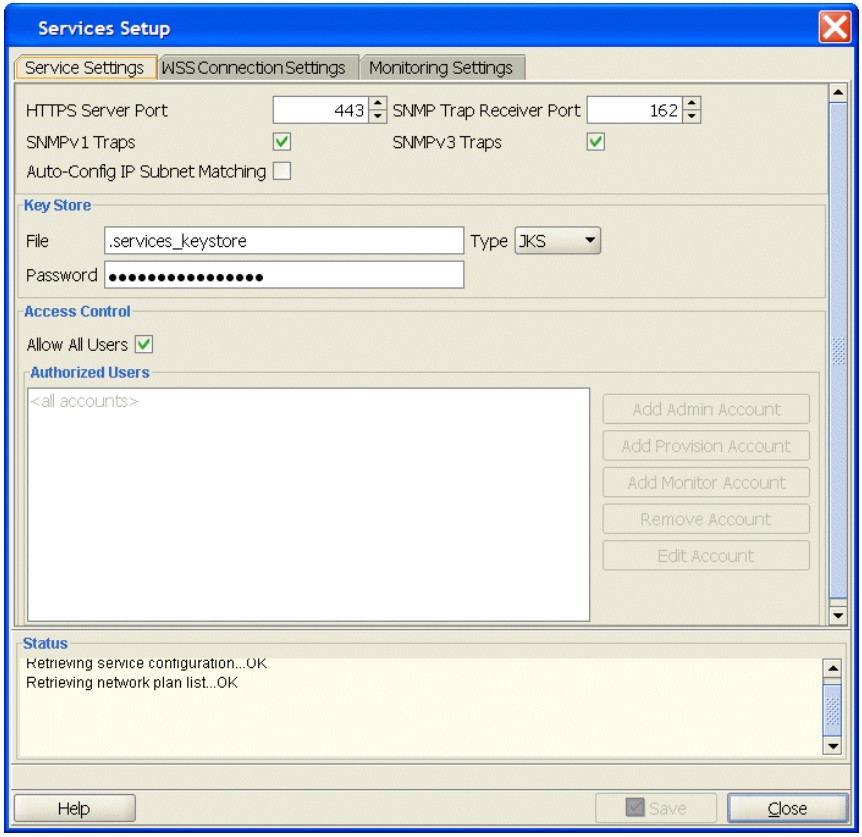
Configure WMS Services

You can change the properties of WMS Services.

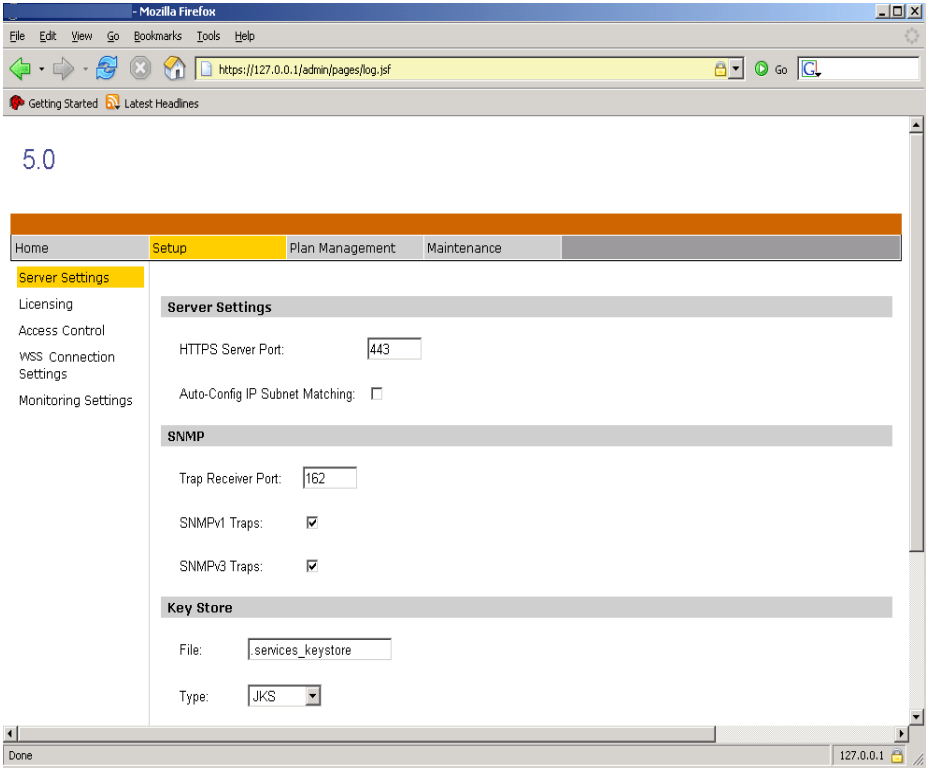
Note. If a firewall is enabled on the host where you install WMS Services, WMS Services will not be able to communicate with WMS client or with WSSs unless the firewall is configured to allow through traffic for the SSL and SNMP ports (443 and 162 by default).

To configure WMS Services

1. Select **Tools > WMS Services Setup** dialog box from the WMS main tool bar. The WMS Services Setup wizard is displayed.



1 Select **Services > Setup.** WMS Services will open in your default Web browser.



By default, a username and password are not required to access WMS Services from WMS client. You can configure user accounts for administrative, provisioning, and monitoring access. (Refer to "WLAN Management Software Access Control" on page 29.)

2 Configure the following options by clicking **Server Settings** on the left of the browser window:

- **Enter the desired HTTPS Server Port in the HTTPS Server Port field. The HTTPS Server Port is the port on which WMS Services listens for requests from WMS client.**
- **Enter the desired HTTP Server Port in the SNMP. The SNMP Server Port is the port on which SNMP traps are received. Select the trap type from which you want WMS Services to receive WSSs, SNMPv1 or SNMPv3.**

Note. On each switch in the network plan, you must enable notifications and configure WMS Services as a notification target (trap receiver).

Note. WMS Services does not start listening for SNMP notifications from switches until you save the network plan.

- **Specify the security settings in the Key Store area.**

The Auto-Config IP Subnet Matching option is used for field replacement of WSSs. For information, refer to "Configuring WSSs Remotely" in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

Click Access Control on the left to define user accounts. For more information about access control, refer to "WLAN Management Software Access Control" on page 29.

To select monitoring settings

All monitoring options are enabled by default. You do not need to enable them and you do not need to specify the switches you want to monitor. However, for WMS Services to receive trap data from WSS switches, SNMP notifications must be enabled and WMS Services must be configured as a notification target on each of the switches.

To start gathering data for monitoring, deploy your configuration to the network. For information about deploying your configuration, refer to "Deploy Your Configuration" on page 162.

WLAN Management Software Access Control

You can create a user account with administrator, provision, or monitor privileges. See Table 4 for basic privilege definitions. For ~~a~~ details, refer to "Restricting Access to WMS" in "Getting Started" of the *Nortel WLAN Management Software 2300 Series Reference Guide*.

Table 4: User Privilege Levels

Privilege Level	Access Control	Configuration	Monitoring
Administrator	yes	yes	yes
Provision	no	yes	yes
Monitor	no	no	yes

To configure access control

1. Select **Services > Setup** from the WMS main tool bar. WMS Services is displayed in your default Web browser**.**
2. Select **Access Control** in the left pane.
3. Click **Enable login-required**. Enter a username and password for administrative access. Click **OK**. (You must configure an admin account before you can configure provisioning or monitoring users.).
4. Enter the name under the Add User section.
5. Select **Administrator**, **Provisioning User**, or **Monitoring User** in the Role field.
6. Enter the password. Re-enter the password.
7. Click **Save**. The new account will appear in the Authorized Users section.
8. To remove an account, click **Delete**.
9. To reset a password, click **Edit**.

WLAN Management Software Interface

This section contains the following topics:

- "Displaying the Main Window" on page 30
- "Using the Toolbar and Menu Bar" on page 31
- "Setting Preferences" on page 31
- "Easy Configuration Using Wizards" on page 32
- "Getting Help" on page 32
- "Getting Help" on page 32

Displaying the Main Window

When you start WLAN Management Software client and log onto WMS Services, a network plan is displayed by the WLAN Management Software client. (See Figure 2.)

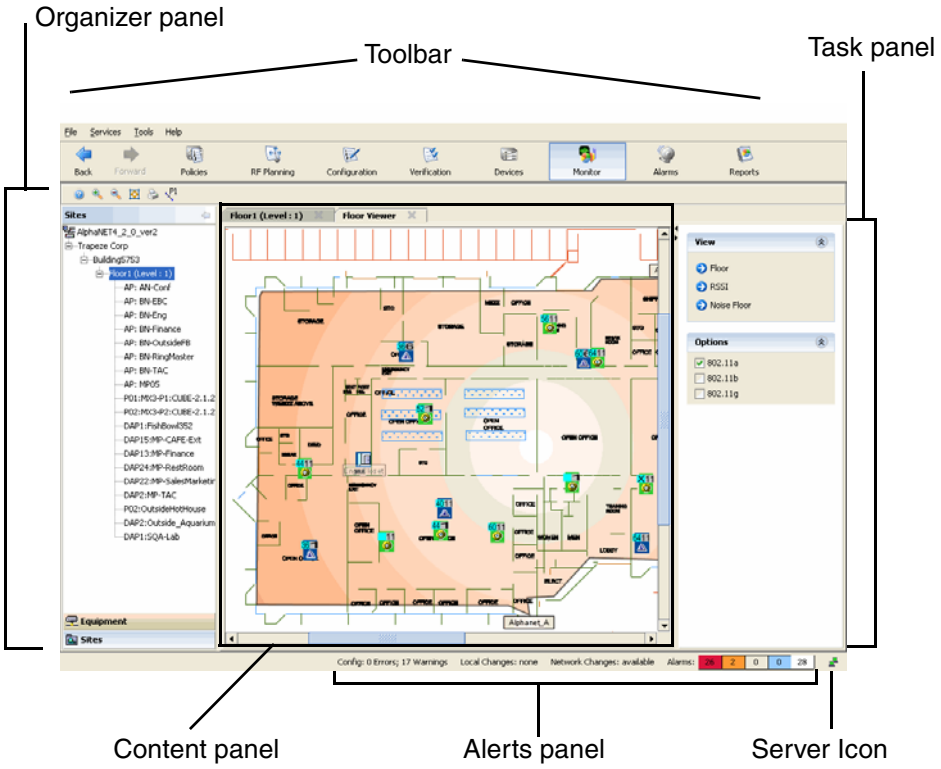
- *Organizer panel* displays a network tree representing your WLAN's devices and configurations on those devices. You can use it to navigate to Policy configurations, Equipment within your network, and network Sites.

  When you select a device or configuration in the tree, the context-sensitive information about the device or configuration is displayed to the right in the Content and Information panels.

- *Content panel* displays context-sensitive information about the device or configuration selected from the tree in the Organizer panel. From the Content panel, view Nortel devices and their status, verify Nortel device configurations in the network plan and in the network, and display event logs and Rogue detection results.
- *Alerts panel* displays a summary of alerts, including network and configuration verification, Rogue detection, and local and network changes. Click on a summary to display details.
- *Task Panel* displays additional context-sensitive options related to your tool bar selection.

The Server icon indicates the status of the connection between the WLAN Management Software client and the host running WLAN Management Software Services.

Figure 2. Main WMS Window with Open Network Plan



Using the Toolbar and Menu Bar

The main WLAN Management Software window has a toolbar that provides quick access to features and summary views. Use the **Back** and **Forward** buttons to cycle through your display selections.

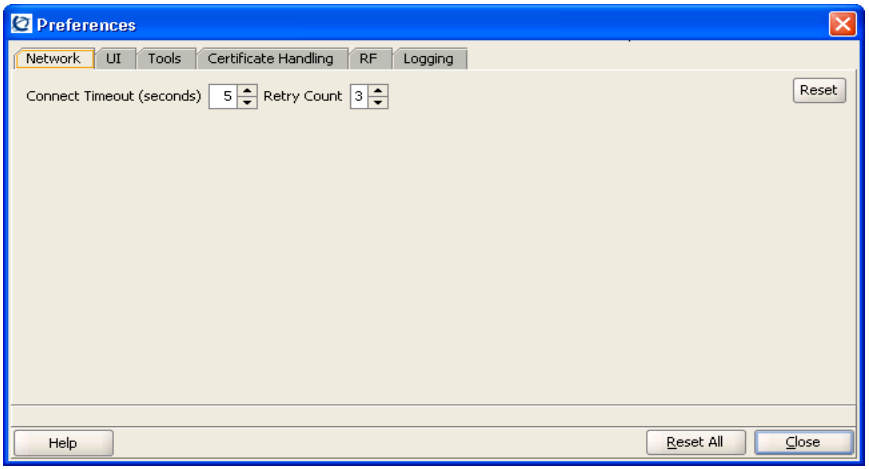
The menu bar (located above the toolbar) provides access to administrative options such as plan management and access to online help. For example, to examine recent activity, select **Tools > Events**.

Setting Preferences

You can set network, user interface, save interval and autosave, certificate handling, RF monitoring, and logging.

1 Select **Tools > Preferences** from the WMS main tool bar.

The Preferences wizard is displayed.



2 Select any of the tabs, make modifications in the fields, and select **Reset All** to reset preferences.

Easy Configuration Using Wizards

Wizards help walk administrators through configuration steps. There are many wizards in the WMS application.

Enter the required fields and click **Next** at the bottom of the wizard to display the next step. Click **Cancel** to discard any changes made with the wizard. When you are done, click **Finish** or **OK** to save changes.

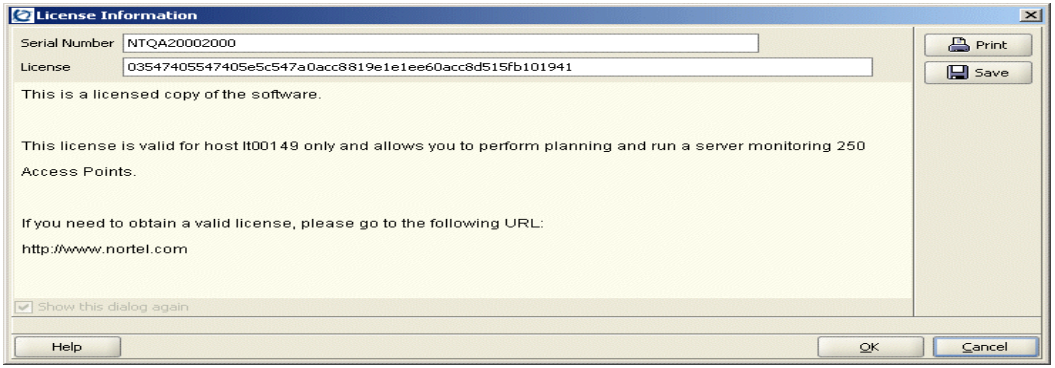
You can right-click on many objects to display the **Insert** option. Select **Insert** to create a new object that is a "child" of the selected object.

Getting Help

Click **Help** from the Main menu bar to access online help and other information:

1 Select **Help > Help** to display HTML help about configuring and using WMS.

2 Select **Services > Licensing** to open a browser window and view product licensing information, or to get access to Nortel product licensing server Web page.


License Information
Serial Number
NTQA20002000
License
03547405547405e5c547a0acc8819e1e1ee60acc8d515fb101941
Print
Save
This is a licensed copy of the software.
This license is valid for host lt00149 only and allows you to perform planning and run a server monitoring 250 Access Points.
If you need to obtain a valid license, please go to the following URL:
http://www.nortel.com
Show this dialog again
Help
OK
Cancel

3 Select **Help > Report Problem** to report a problem to Nortel Technical Support.

Select **Help > About WMS** to display information about WMS. You also can click **Force GC** (garbage collection) to free resources.

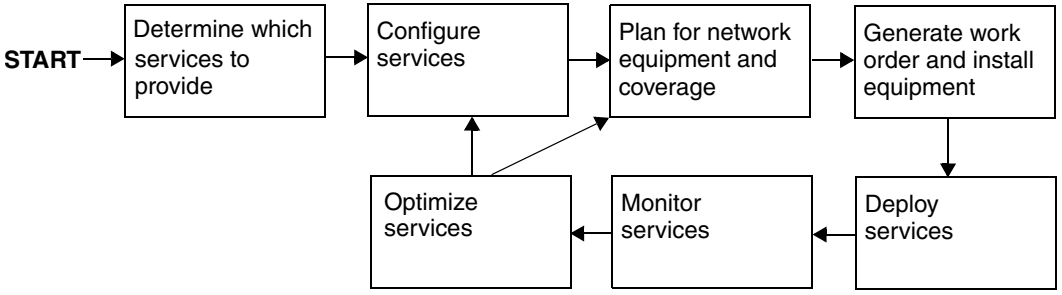
Planning and Managing Your Wireless Network with WMS

Which Services to Provide? 35
Network Plan 36
RF Coverage Area 36
Configuration 39
Equipment Installation 46
Deployment 47
Management and Monitoring 47
RF Plan Optimization 51

This chapter contains information about planning and managing your wireless network with WMS. Planning your wireless network is highly recommended because it not only helps you configure and deploy it, but also aids in scaling and monitoring your network. Nortel provides you with flexible tools to assist with network planning.

Plan your wireless network to support the services you want to offer your employees, guests, or customers. Figure 1 describes the process to establish services in your company or organization, beginning with determining the services you want to offer. Each step in the process is described in this chapter.

Figure 1: Process to Establish Wireless Services



Which Services to Provide?

What is a service?: A service is a concept (not a selectable item in the WMS interface) that represents a set of options you configure and deploy on your wireless network. You configure services to support the different levels of network access you need to provide. For example, a service configured to support employee access will have different

options configured to provide greater access to the network. In contrast, a service configured for guest access typically restricts users to limited or no internal network access, but easily provides a gateway connection to the Internet.

A service can be fully isolated and independent of other services on the network (multi-hosted access is typically isolated), or you can reuse part of a service configuration for another service you want to provide. Each service has potential authentications (802.1X, Web page, MAC address, or "last resort") and potential encryptions (802.11i, WPA, WEP, or unencrypted).

Purpose of this section: To provide information about services that you can configure using WMS.

Why is this important?: Understanding the services you can configure with WMS is the first step in planning and configuring your network.

First, determine which services your organization requires. The three common types of services are as follows:

- Employee access
- Guest access
- Voice over Wireless IP (VoWIP)

Employee access is typically secure, encrypted access to the wireless network. Guest access is access (possibly unencrypted) for visitors at your location. If you intend to resell services to other providers, you will need to provide multi-hosted access.

Determining the services you will need at the beginning of the planning process results in configuration data. The configuration data is used to create service profiles and AAA rules for each service. A *service profile* is a subset of a radio profile. A *radio profile* is a common set of configuration parameters that can be applied to many AP radios.

See "Create a Service Profile" on page 103 for information about configuring services.

Network Plan

What is a network plan?: A network plan is the workspace in WMS you use to design a wireless network.

Why is this important?: You can better manage and visualize your network topology by creating a detailed and accurate network plan.

You can start by creating a device-oriented (WSSs and APs) view of your network without any geographic information about your site—no floor dimensions, building material information, or RF obstacle information. You can go a step further and provide some geographic information by adding floor dimensions, your RF coverage area, and some attenuation information, such as elevator shafts or internal concrete walls. If you want to enjoy the full benefits of network monitoring and visualization, you can create a detailed network plan. This is done by importing detailed building and floor plans into WMS, defining RF obstacles, and defining the quality of coverage (traffic engineering parameters) you want for specific RF coverage areas.

RF Coverage Area

What is an RF coverage area?: An RF coverage area is the geographical area in which IEEE 802.11 radios provide wireless services.

Purpose of this section: To describe the three techniques you can use for RF coverage.

Why is this important?: By understanding available RF coverage planning techniques, you can use the technique that meets your organization's requirements.

The following are three techniques you can use to start your wireless network:

- *Auto-RF* lets you use the default auto tuning feature to select power and channel settings for RF signals in your RF coverage area. You upload the WSSs into WMS, configure the APs, enable Auto-RF, and deploy.
- *Auto-RF with Modelling*, as with the Auto-RF technique, lets you set the auto tuning feature to adjust power and channel settings to provide RF signals to the coverage area for your users. Enhance the auto tuning feature by providing modelling information about your geographic location. By providing some information about your buildings and floors, you add enough details into WMS so that you can better visualize your network topology and support improved monitoring at your site.
- *RF Planning* is a technique you can use to create a detailed network plan that provides powerful monitoring and visualization benefits. Unlike Auto-RF or Auto-RF with Modelling, you do not rely on the auto tuning feature. Instead, you fully model your geographic location with detailed information about your floors and specify your RF coverage areas and your RF obstacles.

Each of these methods is described in the sections that follow.

Auto-RF

Perform the following steps to use the Auto-RF technique:

- Physically place WSSs and the APs in their desired locations.
- Upload a WSS configuration and deploy it.
- Enable the Auto-RF feature.

This is a great way to install a WSS and some APs and observe how the network operates. The Auto-RF plan is best suited to networks containing fewer APs.

Auto-RF with Modelling

To use the Auto-RF with Modelling technique, you add to the Auto-RF technique by providing some geographical modelling about your building, floors, and RF coverage area. You also add RF obstacle information for major obstacles (like concrete walls, windows, and elevator shafts) that affect attenuation—the quality of RF signals emitted from and received by the APs. By adding geographical modelling, you will be able to manage your network in the context of that geographical information. For example, you will be able to manage your network overlaid on a floor plan, versus managing an abstract logical group of switches and APs.

RF Planning

To do RF Planning, you provide detailed information about your site and buildings by importing AutoCAD DXF™, AutoCAD DWG, JPEG, or GIF floor plan files of the buildings into WMS. As you import the floor plans, you can modify them to add or remove RF obstacles. You define RF obstacles by specifying the attenuation factor in decibels for the obstacle. In addition, WMS includes a library of attenuators for building obstacles. The library includes doors, walls, ceilings, and other physical obstructions that you can select. WMS factors in the impact these objects have on how the radio frequency (RF) signals flow through a given site.

If the network contains third-party or pre-installed APs, you can enter information for these APs so that WLAN Management Software takes the APs into account when calculating the placement (and optionally, the channel and power settings) of the Nortel APs.

By using this technique, you receive the following benefits:

- Instead of you making a “best guess” as to how many APs you require for the desired coverage and where APs should be placed, WMS automatically calculates how many APs you need and where to place APs for optimal positioning.
- You can generate a deployable work order to help installers place WSSs and APs.
- You automatically receive a deployable configuration that includes optimum power and channel settings.
- You enjoy more accurate monitoring options and network visualization based on the additional geographic modelling information loaded into WMS.

Note. The RF Planning software does not support outdoor installations. Results obtained do not compensate nor account for obstacles and characteristics typically associated with outdoor environments. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.

Which Planning Method Should I Use?

The more detailed your network plan, the better you will be able to manage and monitor the network. However, there are other requirements that organizations should consider.

Nortel recommends using the Auto-RF technique if you are installing APs without consideration to blanket coverage, throughput concerns, or the number of users for whom service will be provided. Auto-RF is ideal for small areas; for example, coverage that only requires a few APs, or widely dispersed areas in a building, such as conference rooms.

Use the Auto-RF with Modelling technique if you want to better monitor your wireless network in terms of buildings, floors, or coverage areas. You might only be able to locate inaccurate or incomplete building and floor plans (perhaps only a JPEG file), but with even a bit more geographic modelling of your site, you boost your ability to manage and visualize your network.

Use RF Planning when you want to use all the tools provided in WMS to deploy, manage, and monitor your network. You likely have multiple constituencies of users you need to consider; for example, sets of users that are mobile and wireless that have specific throughput and bandwidth needs. One group of users might be mobile and require high throughput performance (a higher bandwidth), while another group of users are more stationary and require less throughput. Additionally, you might be planning for future capacity and need to add as much detailed information as you can about your site in order to plan for the future.

See Table 1 for some guidelines to help you determine what planning technique is right for your organization.

Table 1: Planning Techniques to Use

Concern	If yes, use	If No, use
Do I have adequate time to add geographic modelling and RF obstacle information?	Auto-RF with Modelling	Auto-RF
Can I locate accurate building and floor plans?	RF Planning or Auto-RF with Modelling	Auto-RF with Modelling
Do I need to plan for capacity of users or quality of coverage (traffic engineering concerns) for certain users?	RF Planning	Auto-RF or Auto-RF with Modelling
Do I need to visualize coverage accurately?	RF Planning	Auto-RF or Auto-RF with Modelling
Do I need to locate users?	RF Planning or Auto-RF with Modelling	Auto-RF
Do I need to locate rogue APs?	RF Planning or Auto-RF with Modelling	Auto-RF
Do I want to better monitor my wireless network in terms of buildings, floors, or coverage areas?	RF Planning or Auto-RF with Modelling	Auto-RF

If RF Planning does not fit your requirements now, you can always use the RF Planning technique in the future when you have the need, the time, and the necessary floor plans available. You also can leverage the data in Auto-RF and convert these RF measurements to configured baseline values for planning.

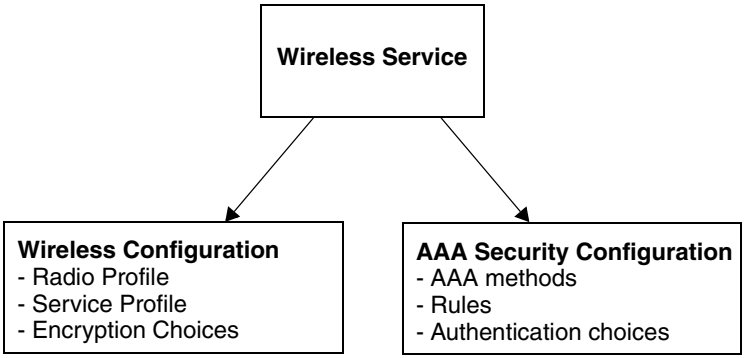
Configuration

Purpose of this section: To describe the main areas of the Nortel (WSS and APs) you will configure in WMS.

Why is this important?: To provide you with overview information about the software so that you can plan a configuration to support the services you require.

You will configure the wireless configuration and AAA security configuration for each service you provide on your wireless network. You also create a basic configuration for the WSS.

Figure 2: Configuration Required for Each Service



This section contains following information:

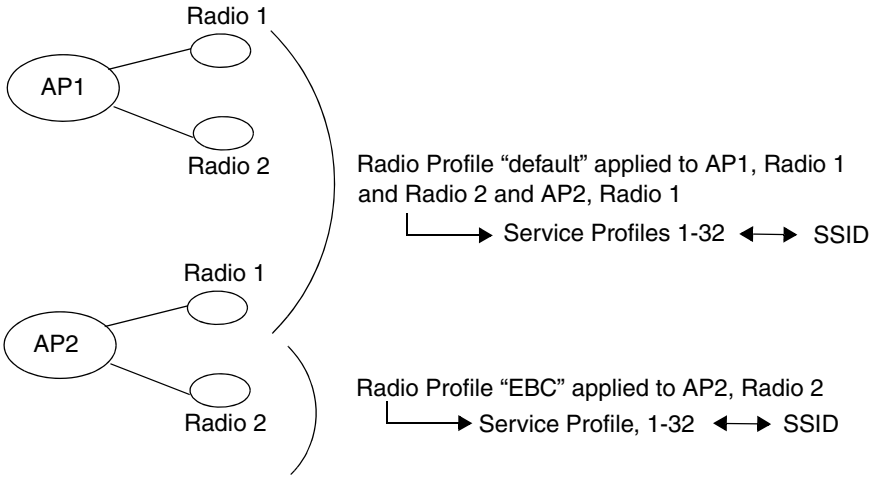
- "Wireless Configuration" on page 40
- "AAA Security Configuration" on page 42
- "System and Administration Configuration" on page 45

Wireless Configuration

Wireless configuration focuses on the configuration tasks (radio configuration and AAA configuration) you do to deliver the virtual wireless services you want to provide on your network. You enable the APs to operate according to your planned RF coverage requirements. Most of the wireless configuration is done as you plan your RF coverage and create your radio profiles and service profiles.

A radio profile is used to apply common settings to multiple radios, and each radio profile can support up to 32 service profiles, one for each service you want to support. You specify in the service profile an SSID for each service and the type of encryption mechanisms to be used by the AP radios. This gives the radio the potential to look like 32 different and independent APs. (See Figure 3.)

Figure 3: Radio and Service Profiles



You must configure a radio profile to set attributes that you can apply to multiple radios. Rather than configuring each radio individually, you create a radio profile and apply it to multiple radios that you select. You can also create a radio profile as part of a policy and apply it to AP on different WSSs.

The radio profile can contain Auto-RF settings and IEEE 802.11 settings that control how the data is received and transmitted. You can select Auto-RF in the radio profile to apply AutoRF settings (enable or disable auto tuning of power and channels) to radios en masse via the radio profile. AutoRF enabled through the radio profile to multiple radios can be easily disabled as well, should you want to go to full RF planning. You can set specific IEEE 802.11 settings, such as beacon, DTIM intervals, and the fragment threshold to control how packets are transmitted.

Note. A default radio profile named *default* is provided and cannot be deleted.

For each service you want to provide, configure the following items in a service profile:

- The SSID name
- SSID advertisement (whether the SSID name is beaconed)
- Whether the SSID name is encrypted or clear (not encrypted)
- Web page (if using Web-based AAA)
- Multiple encryption choices (Dynamic/static WEP, WPA, WEP + WPA, 802.11i)

Note. You also must configure AAA security configuration items for each service. For more information, refer to “AAA Security Configuration” on page 42.

The encryption type you use depends on the type of services you are offering. Employee access is typically encrypted, guest access is typically clear (no encryption) and multi-host or “multiple virtualized services” service can be encrypted,

with each SSID being matched with its own service profile. If services are being used for customer corporate entities (e.g. different airlines on an airport wireless net), then they would probably use 802.1X and strong encryption with Web guest access for their airport club guests. If the services are being used to advertise multiple wireless service providers (WISP), such as T-Mobile™, Wayport ®, and Boingo Wireless™, then these services would probably be completely open. However, they would likely be assigned to their own dedicated subnet containing their proxy server/billing gateway.

AAA Security Configuration

An administrator can control the way in which users access the network. For each service you provide, you can configure unique authentication, authorization, and accounting (AAA) security features, creating an entirely virtualized wireless service. For each service, configure the following items:

- Multiple authentication choices (802.1X, Web, AAA, MAC authentication, Bonded Auth, open)
- AAA methods (up to four RADIUS server groups, or a local database on the WSS)

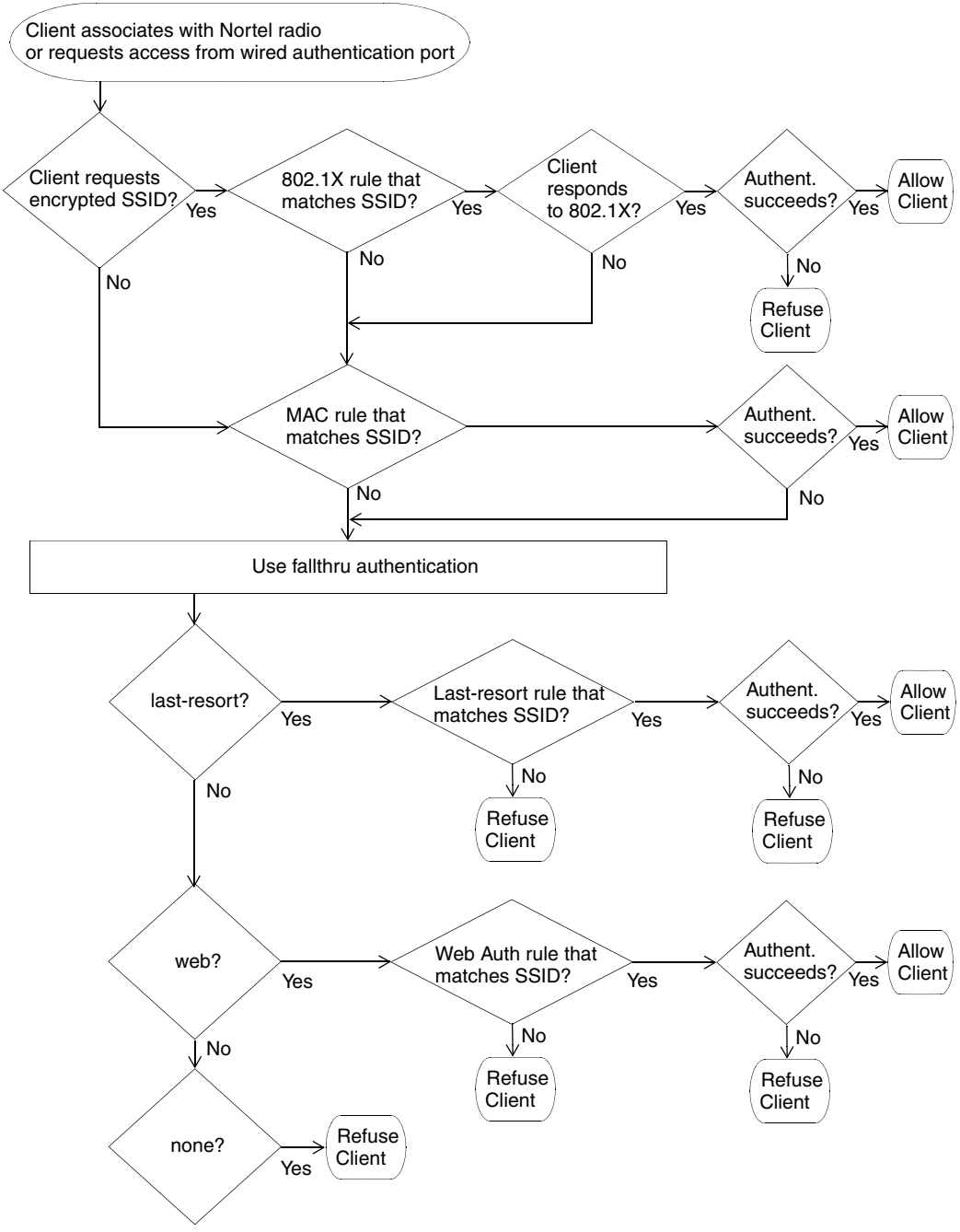
Authentication

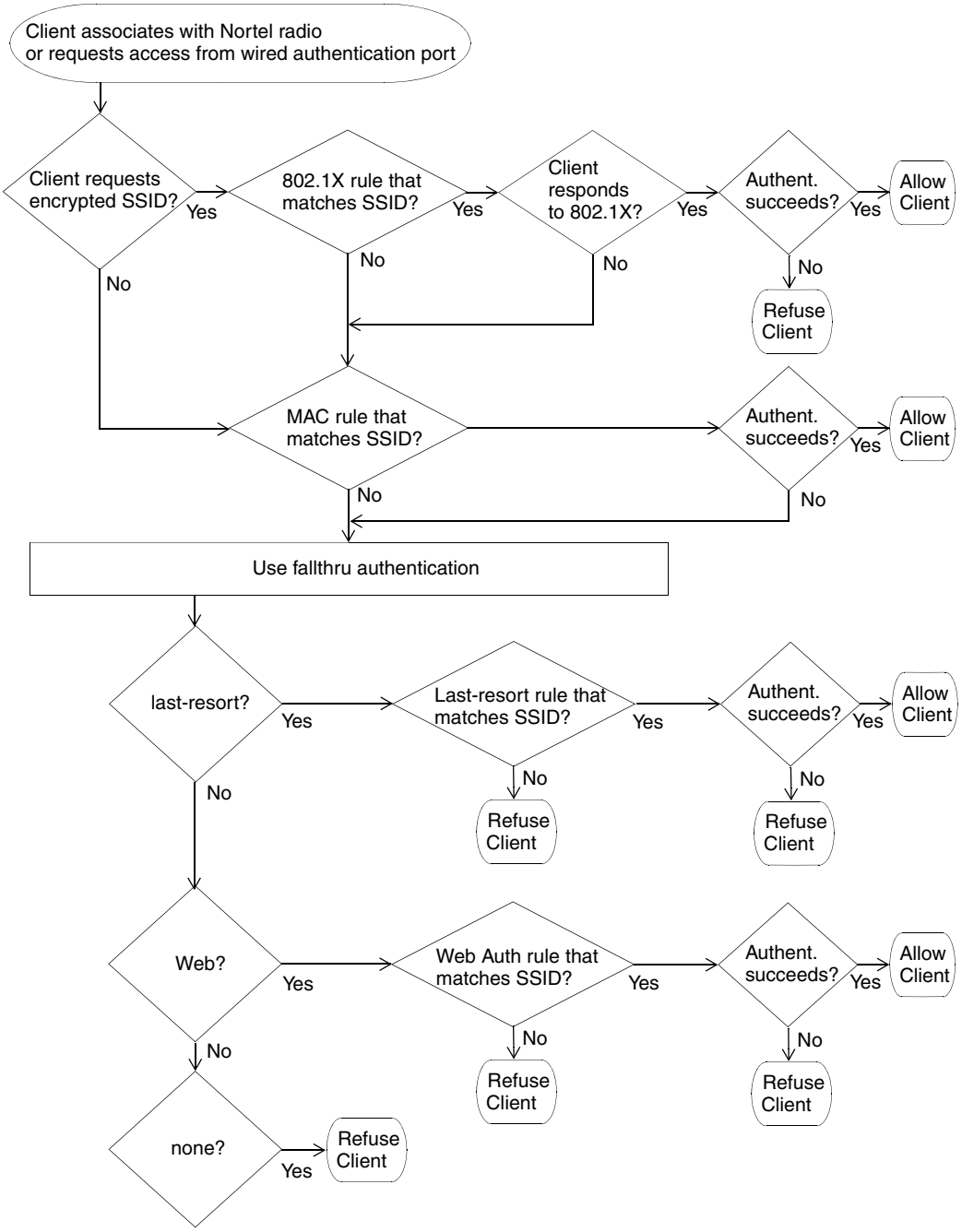
Authentication is the method of determining whether a user is allowed access to your network. Users can be authenticated by a RADIUS server (pass-through) or by the WSS local database (local). The WSS can also assist the RADIUS server by performing the Extensible Authentication Protocol (EAP) processing for the server (off load).

To authenticate users, you will need to configure users either in the local database or on RADIUS servers. Each user will have a username, password, and RADIUS and/or vendor-specific attributes (VSAs). You will also need to configure authentication rules (802.1X, MAC, last-resort, or Web authentication).

See Figure 4 on page 43 to view a flowchart representing the authentication process. Generally, 802.1X authentication is attempted first. If the user fails, then MAC authentication is attempted. If this fails, then last resort and Web authentication is used. For a service profile, you specify *either* Web authentication, last-resort, or none in the auth-fall-thru box. You can only select one.

Figure 4: Authentication Flowchart for Network Users




Client associates with Nortel radio or requests access from wired authentication port
Client requests encrypted SSID?
Yes
No
802.1X rule that matches SSID?
Yes
No
Client responds to 802.1X?
Yes
No
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
MAC rule that matches SSID?
Yes
No
Authent. succeeds?
Yes
No
Allow Client
Use fallthru authentication
last-resort?
Yes
No
Last-resort rule that matches SSID?
Yes
No
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
Refuse Client
Web?
Yes
No
Web Auth rule that matches SSID?
Yes
No
Authent. succeeds?
Yes
No
Allow Client
Refuse Client
Refuse Client
none?
Yes
Refuse Client

Authorization

Authorization is the method for providing users with specific rights to the network by associating attribute-value (AV) pairs to the user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a local database or on a RADIUS server for a given user and the result is returned to the WSS to determine the user's actual capabilities and restrictions.

You can configure attributes, such as the time of day or specific VLAN access. You can also control access using security access control lists (ACLs), Mobility Profiles™, and Location Policies. Security ACLs permit or deny traffic based on IP protocol, IP addresses and, optionally, TCP or UDP port. They also can be used to set class-of-service (CoS) values in a packet. Mobility Profiles contain attributes to allow or deny access to specific parts of the network for a specific user or group of users. Location Policies are an ordered list of location policy rules based on a user glob, VLAN, and/or ports. A Location Policy can be configured if you need to override the configured AAA user authorization attributes locally for a specific WSS.

Accounting

Accounting collects and sends information used for billing, auditing, and reporting—for example, user identities, connection start and stop times, the number of packets received and sent, and the number of bytes transferred. You can track sessions through accounting information stored locally or on a remote RADIUS server. As network users roam throughout the network, accounting records track them and their network usage.

System and Administration Configuration

A Mobility Domain is a collection of WSSs that work together to support roaming users. One of the WSSs is defined as a seed device, which distributes information to the other WSSs defined in the Mobility Domain.

A Mobility Domain allows users to roam geographically from one WSS to another without losing network connectivity. Users connect as a member of a VLAN through their authorized identities.

You can add switches to a network plan as members of a Mobility Domain or as standalone switches. After a switch is added, you can move it into or out of a Mobility Domain.

You can create the following kinds of switches:

- 2382 —Provides two gigabit Ethernet ports. Each port has a miniature Gigabit interface converter (mini-GBIC) slot for insertion of a small form-factor pluggable (SFP) 1000BASE-SX or 1000BASE-LX fiber-optic interface. One 10/100 Ethernet port for out-of-band management (without PoE).
- 2380 —Provides four dual-interface gigabit Ethernet ports. Each port has a 1000BASE-TX copper interface and a Gigabit interface converter (GBIC) slot for insertion of a 1000BASE-SX or 1000BASE-LX fiber-optic interface.
- 2360—Provides eight 10/100 Ethernet ports, six of which support PoE.
- 2350 —Provides two 10/100 Ethernet ports, one of which supports PoE.

Perform the following tasks to create and initially configure a WSS:

- Configure basic WSS properties.
- Configure WSS connection information.
- Configure boot information.

Configure Basic WSS Properties

To configure basic WSS properties, you specify a name, select a model, select its location by wiring closet, and select the WLAN 2300 System Software (**WSS Software**) you want to run on the switch. Optionally, you can select a **WSS Software** image to download when you deploy changes to the WSS.

You also can specify if the switch is managed. A WSS that is physically installed as well as configured can be managed. You can deploy configuration changes only to managed devices, and WMS periodically checks the managed WSSs in the network for changes. You also can fully configure a switch without it being physically installed (unmanaged). Having an unmanaged device in your network plan might be useful for predeployment purposes.

Basic configuration also includes specifying how you will manage the switch. You can manage it through HTTPS, Telnet, and Secure Shell (SSH). You also can enable monitoring using the Simple Network Management Protocol (SNMP) to exchange information about network activity between your network devices.

For more information about configuring basic WSS properties, refer to "Perform Basic Administrative Tasks" on page 163.

For detailed information about configuring basic WSS properties, refer to the *Nortel WLAN 2300 System Software Quick Start Guide*.

Configure WSS Connection Information

You need to supply connection information for the WSS on both the WSS and in WMS when you make the WSS a managed device. Connection information includes the IP address of the switch and how it will connect to the backbone; for example, by means of a VLAN or a port.

Configure Boot Information

You select the software image that the WSS will use when reset, or optionally, the configuration file the WSS will use when reset.

Equipment Installation

Perform the following steps to physically install a WSS:

1. Unpack and rack the WSS in the wiring closet or data center location.
2. Plug the WSS electrical cord into a power outlet.
3. Connect a network access cable from your existing network to one of the Ethernet ports on the switch (10/100 or Gigabit Ethernet, depending on the WSS model and available interfaces on the network).

Note. Remember the port number you used. You will need to know this when performing the initial setup of the switch.

4. Connect a serial interface to the console port of the WSS to access the console's CLI for initial setup.

Perform the following steps to physically install APs:

1. Instruct the cabling installer to run the Cat. 5 Ethernet cable from the closest wiring closet to intended location of the AP.
2. Unpack the AP and select the appropriate mounting kit for your installation location.
3. Install the AP at the indicated location on the floor.
4. Connect the Cat 5. Ethernet cable(s) to the AP.
5. At the wiring closet, connect the AP to the infrastructure equipment as follows:
   a. If you are directly connecting the AP to a WSS, plug the other cable end(s) to the indicated port(s).
   b. If you are indirectly connecting the WSS to the switch, plug the other cable end(s) to an available network port on the wiring closet switch. If the switch does not supply PoE, then ensure that a mid-span PoE device is inserted in-line with the connection.

Deployment

What is deployment?: Sending the WSS configuration information in the WMS network plan to your WSS.

Purpose of this section: To describe how changes are made to WMS and deployed to your network.

Why is this important?: To understand best practices for sending and deploying configurations to your WSS.

Configuration changes are collected in WMS when you save them, but are not applied to WSSs until you send the changes to your network. Any changes you make to your network in WMS are saved, but not applied to your network until they are deployed. This method makes it easy to apply configurations simultaneously to multiple WSSs, or you can deploy changes to a single WSS.

Management and Monitoring

Purpose of this section: To provide an overview of the management and monitoring capabilities offered in WMS.

Why is this important?: Understanding the management and monitoring tools available in WMS can help you to quickly identify and correct problems in your wireless network, as well as to provide you with the statistics and reporting information you need to optimize your network.

This section talks about the following management and monitoring features:

- Network Status
- Client monitoring
- Fault management
- Rogue detection
- Event logging
- Verification
- Reporting

Network Status

WMS provides summary status on devices in the network at the Mobility Domain, switch or AP level. View the summary status as the initial step in monitoring. Summary status displays the operational status of WSSs, AP, and their radios (whether they are up or down).

In addition, WMS collects network statistics for devices, including system-level events and statistics for the wired network.

The Alerts panel at the bottom of the WMS window displays top-level status information. The Alerts panel provides you with summary error and warning information for the following areas:

- Config—indicates network plan configuration issues
- Local changes—indicates changes in WMS that can be deployed to the network
- Network changes—indicates configuration changes in the network
- Alarms—shows the number and severity of alarms detected in the network

RF Monitoring

RF monitoring provides you with current and historical information about your radio health and activity.

Statistics collected for the RF environment provides data on a per-channel basis. You can view noise levels, cyclic redundancy check (CRC) and PHY errors, packet retransmissions and percent utilization.

Data collected for the RF neighborhood displays the neighboring radios. This information can be viewed as a list of radios heard by a particular radio, as well as a list of radios who can hear a particular radio.

You also can display trending information on a per-radio basis. Trending collects radio statistics and charts them on a time basis. For example, you could display average throughput rates for the previous 30 days, week, or day. You can display and print the charts from WMS, as well as generate a report.

Client Monitoring

Client monitoring provides current and historical information about the clients using your network, including client activity, current client sessions, and the ability to locate clients at your site. WMS displays the data that WSSs collect on user sessions—either for a single user, users associated with an AP, or users associated with a specific radio.

By viewing monitoring information for a user or a group of users, you can troubleshoot problems originating from bandwidth constraints or roaming patterns. You can collect statistics and view reports about the following:

- Client associations, authentication, and authorization failures
- Client activity, such as roaming and successful authorization
- Current session status, location history, and statistics
- Specifics on users over a period of time; information can be gathered up to 30 days for session status, location history, and client errors

If you use WLAN Management Software RF Planning, you also can display the approximate geographic locations of clients.

Fault Management

The Fault Management System is a feature included in WMS to make it easier to manage faults (alarms) that occur in the network. A fault or alarm (these two terms are used interchangeably) is generated by a trap, a rule, a status, or a threshold-exceeded event. The Fault Management System monitors traps from Nortel and OEM devices.

The Fault Management System also monitors certain traps for third-party applications, and offers administrators the ability to add new trap support when necessary. The type of trap and IP source determine how new trap support should correlate with existing trap support.

WMS incorporates a powerful and flexible display interface for all alarms collected by the system. Alarms are stored on a per-WSS basis and are collected continuously. Create custom filters to drill down to specific information in the event log database. You can filter alarms based on the following:

- Category
- Severity
- Date and time ranges
- WSS
- WMS client and services log
- Specific text string matches

Rogue Detection

A rogue AP is an access point that is not authorized to operate in or near your network. You can use the Fault Management System to identify and locate rogues in your network, and then use RF countermeasures to deny service to or from a targeted rogue AP, rendering them ineffective. Once a rogue AP is detected and reported, the closest Nortel AP is assigned to perform RF countermeasures. By spoofing various 802.11 control messages, the AP's countermeasures disrupt association and authentication attempts to the rogue AP by any new clients. This also disrupts any active communications between any existing client and rogue AP.

The Fault Management System allows you to collect statistics and view reports about the following:

- Current rogue list, aggregated for the whole network
- Current hour rogue list
- Current day rogue list
- 30 days of rogue history, using best listener data
- Rogue lifecycle events (when the rogue was first seen, by whom, and when it went away)
- Counter-measure activity

Verification

Both configuration verification and network verification rules are checked for any inconsistencies or problems. Verification rules include "instant fix" resolutions. Instant fix resolutions are errors that can be automatically fixed, or alternatively provide a hot link to the object containing the error.

You can selectively disable any rule. Disabling a rule is useful if you wish to ignore a warning and do not want it to display. Reporting

WMS uses a database to collect and store client, RF, and other system dynamic data, such as statistics, status, events, and traps. You can generate reports from the monitoring and configuration data collected in the database. A report can have a selectable scope and a selectable time period and in some cases, query filter parameters. See Table 2 for a listing and description of the reports you can generate in WMS.

Table 2: WMS Reports

Report	Description
Configuration Reports	
Inventory Report	Provides information about the WSSs and APs in your network.
Mobility domain configuration	Provides a configuration overview, providing data that spans multiple WSSs. For example, it contains information about the AAA/RADIUS setup, SSIDs, and where they are configured.
WLAN—Security Switch (WSS) Configuration	Provides details on a WSS configuration.
Client Monitoring Reports	
Client Session Summary	Displays summary data for sessions in the selected scope.
Client Session Details	Displays detailed session information.
Client Errors	Provides data on client-related health in the network over time; for example, if there is a large number of association failures in some area of the network.
RF Reports	
Wireless Network Usage	Provides information about network resource usage and client activity.
RF Summary	Provides information about overall network health using selected radio statistics. It can be used to compare RF environments across the network and isolate potential problem areas.
Radio Details	Provides a detailed set of statistical information for each radio in the selected AP.
Traffic Reports	
Traffic	Provides details about the throughput rate and types of packets passing through the network.
Rogue Reports	
Rogue Details	Provides current and historical information for a selected rogue.
Rogue Summary	Provides information for all visible rogues for a selected time.
RF Planning Reports	

Table 2: WMS Reports (continued)

Report	Description
Site Survey Order	Provides a map of your site that can be used to guide a site survey.
Work Order	Provides information installers use to physically install WSSs and APs.
Alarm Reports	
Alarm Summary	Provides the total number of current faults in the system and identifies them by type, source, severity or state.
Alarm History	Provides a list of all faults in the system that were active within a specified time period. Users can sort the faults by source, severity, or category.
Security	Provides a report of Denial of Service (DoS) and Intrusion Detection System (IDS) alarms.
Client OUI	Provides a list of alarms according to the Organizationally Unique Identifier (OUI) of the client for which the alarms were generated.

RF Plan Optimization

What is optimization?: Importing RF measurement data into an RF model to improve the accuracy of the model.

Purpose of this section: Provides an overview of optimization methods.

Why is this important?: A network plan contains the configuration settings that determine the performance of your wireless network. Optimization of the RF model leads to a more successful RF plan. The ultimate result is an accurate visualization of your RF coverage, better-defined statistics for monitoring, and the ability to more accurately plan for and improve network performance.

You can optimize your network based on user and network statistics gathered from:

- The monitoring data in WMS
- A site survey

Based on RF measurement data you gather in WMS to optimize the RF model of a floor, you can make configuration changes in the software to improve signal strength and coverage for groups or individuals, modify AP locations, or add additional equipment to your wireless network if statistics indicate your network has outgrown the support provided by its current deployment of WSSs and APs.

You also can import RF measurement data based on a site survey done outside of WMS. Refer to "Optimizing a Network Plan" on page 201 for general guidelines about performing a site survey.

Configuring Wireless Services

What Are Services? 53
Configure Employee Access Services 54
Configure Guest Access Services 69
Configure Voice over Wireless IP Service 85
What's Next? 100

What Are Services?

A service is a concept that represents a set of options you configure and deploy on your wireless network; it is not a selectable item in the WMS interface. Services are configured to provide various levels of wireless network access to users, such as secure employee access, guest access, multi-hosted access, or Voice over Wireless IP (VoWIP) access.

You can configure a service to be independent of other services on your wireless network, or you can share configuration components among services. For example, multi-hosted access is typically fully isolated from other services (no shared configuration), while services that provide for guest and employee access in a single corporation might share a common radio profile. In this way, you can reuse part of the service configuration for other services you want to provide. You could configure a service for employee access; then reuse part of the configuration to provide services for guest access.

Each service has potential authentication types; for example, 802.1X, Web page, MAC address, or open access. Open Access is sometimes called *last resort.* Each service also has potential encryption types, such as 802.11i, WPA, WEP, or unencrypted.

This chapter contains examples to help you configure the following types of service sets:

- Employee access (802.1X)
- Guest access (Web Portal)
- Voice over IP (MAC AAA)

Note. The configuration examples in this chapter take place on a WSS already in the network plan. However, you also can preconfigure services in a policy and apply the policy to WSSs later.

Configure Employee Access Services

Services for Employee access are typically configured to provide secure, encrypted access to the wireless network.

The following sections provide information about how to configure Employee access:

- "Task Table" on page 54
- "Step Summary" on page 56
- "Example: Configure Employee Access" on page 56

Table 1 on page 54 contains the tasks you need to configure Employee access services. The summary provides the configurable options you should set. Refer to "Example: Configure Employee Access" on page 56 for information about the primary wizards and pages in WMS that allow you to configure Employee access services.

Task Table

Table 1 contains the tasks you need to perform to create a service for employee access. For a summary of configurable items, refer to "Step Summary" on page 56. For detailed steps about how to perform each of these tasks, refer to "Example: Configure Employee Access" on page 56.

Table 1: Creating a Service for Employee Access

Task	Path	Primary Parameters to Configure
"Create a Radio Profile" on page 57	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click on Radio Profiles. 5. Select Radio Profile in the task list.	From the Create Radio Profile wizard: • Radio profile name: Enter a name After you create the service profile, you can map it to the radio profile. After you install the APs, you can map their radios to the radio profile. **Note:** The examples in this chapter configure the radio profile first. However, you also can configure the radio profile later as part of service profile configuration.

Table 1: Creating a Service for Employee Access (continued)

Task	Path	Primary Parameters to Configure
"Configure RADIUS Servers" on page 58	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand AAA. 4. Click RADIUS. 5. Select RADIUS Server in the Task List.	From the Create RADIUS Server wizard: • Name: Enter server name • IP Address: Enter server IP address • Key: Enter key • Server group: Allow the wizard to create it On the RADIUS servers themselves, configure the AAA backed (not in WMS): • Set up each WSS as a RADIUS client. • Define the Nortel vendor-specific attributes (VSAs) in the RADIUS server's dictionary. • Configure each user record with authorization rules (username and password). • Configure each user with either the Vlan-Name attribute (Nortel VSA) or the RADIUS Tunnel-Private-Group-ID to assign users to VLANs. • Configure authentication rules (802.1X, MAC, Open Access, or Web Portal).
"Create a Service Profile for 802.1X Access" on page 62	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click Wireless Services. 5. Select 802.1X Service Profile in the Task List.	From the Create Service Profile wizard: • Service profile name: Edit name • SSID name: Enter name • Security mode: Select WPA (and deselect Dynamic WEP) • Encryption type: Use TKIP (already selected) • EAP Type: Use External RADIUS Server (already selected) • RADIUS server group: Select one • SSID default VLAN: Enter name • Radio profile: Select one
"Set Up VLANs on WSSs" on page 66	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand System. 4. Click VLANs. 5. Select VLAN in the Task List.	From the Create VLAN wizard: • VLAN Name: Enter name • VLAN ID: Select number • IP Address: Enter IP Address • Ports: Select ports and either move (use only in the new VLAN) or add them (share with other VLANs) • If you add ports, select Tag

Step Summary

The following list summarizes the fields selected or configuration items entered to configure Employee access:

1. Create a radio profile.
   - **From the Radio Profile wizard, enter *RadioProfile1* as the name of the radio profile.**
   - **Click Finish.**
2. Configure the RADIUS back end.
   - **Configure the RADIUS server for 802.1X. Use the recommended EAP method, PEAP + MS-CHAPv2.**
   - **Set up each WSS as a RADIUS client.**
   - **Define any desired Nortel vendor-specific attributes (VSAs).**
   - **Configure each user record with either the VLAN-Name attribute or the RADIUS Tunnel-Private-Group-ID.**
   - **Configure 802.1X authentication rules.**
3. Configure the RADIUS server in WMS.
   - **From the Create RADIUS wizard, enter *sg1* as the Name of the server, the server's IP address, and the Key. Allow the wizard to create the server group and place the server in it for you. Click Finish.**
4. Create a service profile for 802.1X service.
   - **From the 802.1x Service Profile wizard, click Next and enter *Secure-802.1X-Employees* as the Name of the service profile and *Employees* as the SSID.**
   - **Click Next. Select WPA and deselect Dynamic WEP.**
   - **Click Next. Leave TKIP enabled.**
   - **Click Next. Leave External RADIUS Server enabled. Select the RADIUS server group and click Add.**
   - **Click Next. Enter *vlan-mkt* as the default VLAN to use if the VLAN is not assigned by RADIUS authorization.**
   - **Click Next. Select *RadioProfile1* and click Add. Select *default* and click Remove.**
   - **Click Finish.**
5. Set up a VLAN on the WSSs.
   - **From the Create VLAN wizard, enter *vlan-mkt* as the VLAN name.**
   - **Click Next. Select the VLAN ports. Click Add to share them with other VLANs or Move to use them exclusively in this VLAN. If you click Add, then select Tag.**
   - **Click Finish.**

Example: Configure Employee Access

The following detailed steps provide an example of how to configure Employee services

- "Create a Radio Profile" on page 57
- "Configure RADIUS Servers" on page 58

- "Create a Service Profile for 802.1X Access" on page 62
- "Set Up VLANs on WSSs" on page 66

In general, these same steps are required to configure other services, too. You can refer to this section, using the summary list or the task table, with configuration options for "Configure Guest Access Services" on page 69 or "Configure Voice over Wireless IP Service" on page 85.

Create a Radio Profile

Configure a radio profile to set attributes that apply to multiple radios. Rather than configuring each radio individually, apply the radio profile to multiple radios. Service profiles are mapped to radio profiles.

The radio profile can contain Auto-RF settings and IEEE 802.11 settings that control how the data is received and transmitted.

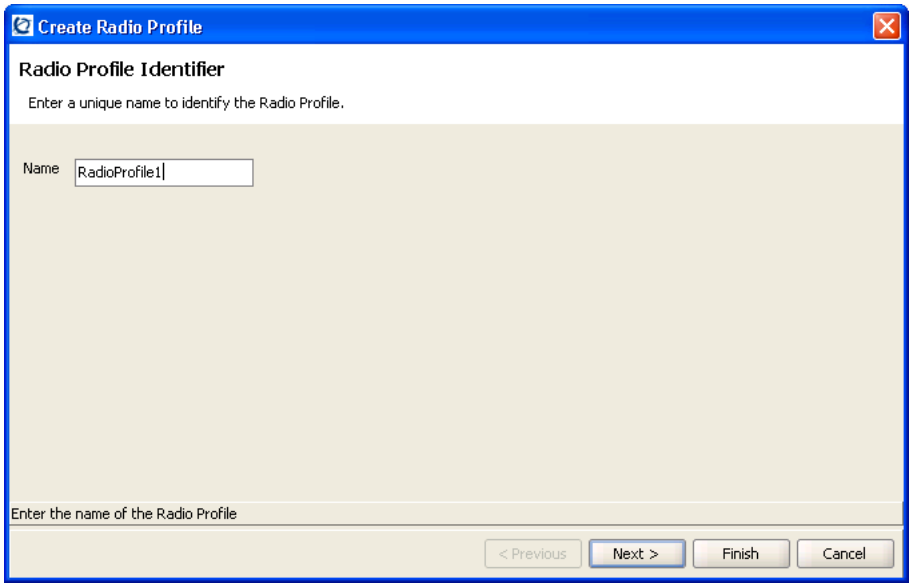
APs (and consequently, radios) need to be added to WMS after creating a radio profile. For more information about adding radios, refer to one of the following:

- "Using Auto-RF" on page 101
- "Using Auto-RF with Modelling" on page 109
- "Using RF Planning" on page 129

To create a radio profile

1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand Wireless, then select Radio Profiles.
4. In the Task List panel, select Radio Profile.

The Create Radio Profile wizard appears.



5 Enter the name of the radio profile, then click **Next** at the bottom of the wizard.

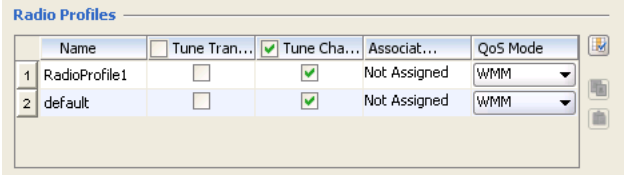
6 If APs are already configured, select the radios to map to the radio profile, then click **Move**.

WLAN Management Software removes the radios from the radio profile they are in and places them in the new profile.

If you have not configured the APs in WLAN Management Software yet, no radios are listed. You can map the radios to the radio profile later.

7 Click **Finish** to save the changes and close the wizard.

The new radio profile appears in the Content panel.



Configure RADIUS Servers

Remote Authentication Dial-In User Service (RADIUS) is a client-server security protocol that provides authentication, authorization, and accounting for network users and devices. A RADIUS server stores user profiles, which include user-names, passwords, and other user attributes.

Perform the following to configure RADIUS servers:

- Configure RADIUS server attributes in WMS
- Configure attributes on the RADIUS server

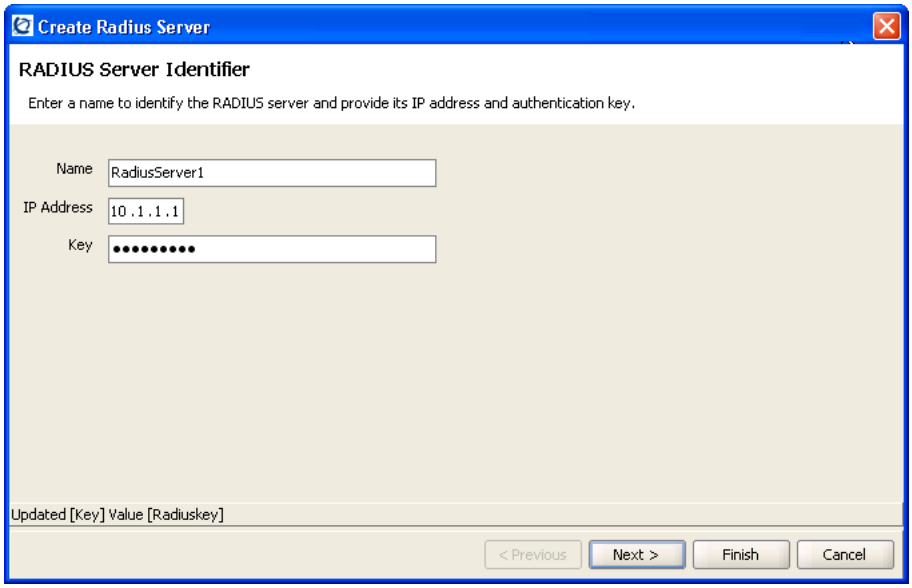
Configure RADIUS Server in WMS

To configure RADIUS in WMS, define RADIUS server groups (named sets of RADIUS servers). You must create at least one server group. RADIUS server groups can authenticate administrators and network users.

To configure the RADIUS server in WMS

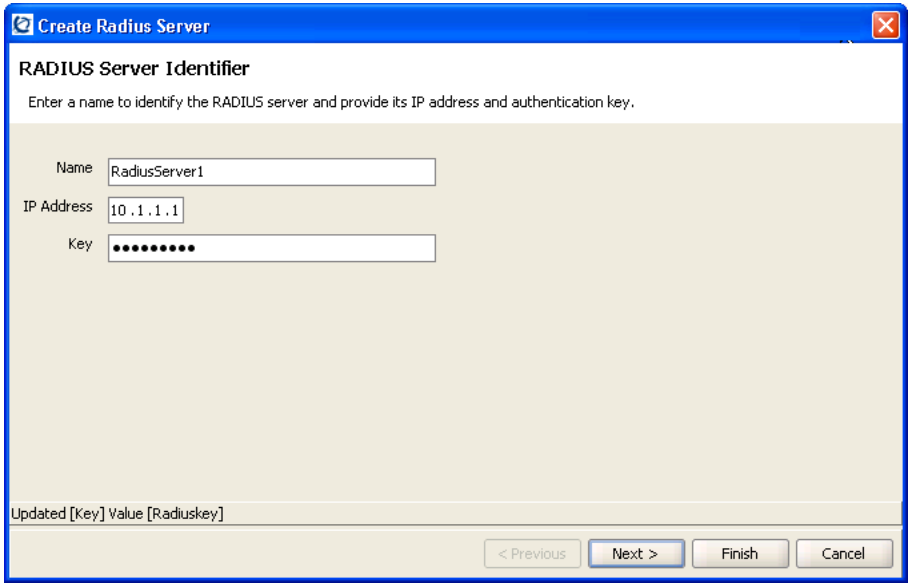
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS on which you are configuring the service.
3. Expand AAA, then select RADIUS.
4. In the Task List panel, select Create RADIUS Server.

   The Create RADIUS Server wizard appears.



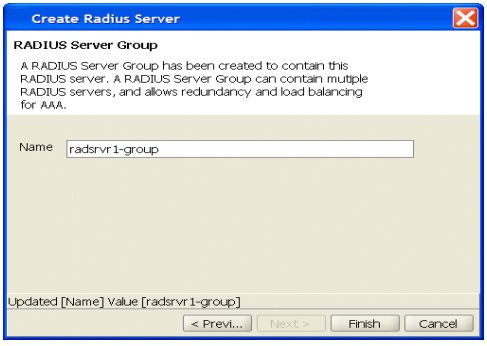
5. Type the name, IP address, and key. Click **Next**.

   WLAN Management Software suggests the name of a server group in which to place the server. The server group is required because AAA rules refer to server groups, not to individual servers.



6 Click **Finish** to save the server and create the server group.

The new server and group appear in the Content panel.


Create Radius Server
RADIUS Server Group
A RADIUS Server Group has been created to contain this RADIUS server. A RADIUS Server Group can contain mutiple RADIUS servers, and allows redundancy and load balancing for AAA.
Name
radsrvr1-group
Updated [Name] Value [radsrvr1-group]
< Previ...
Next >
Finish
Cancel

Configure Attributes on the RADIUS Server

To authenticate users, configure users either in the local database or on RADIUS servers. To configure services for Employee access, configure the following items configured on the RADIUS server.

To configure the RADIUS server

1 Configure RADIUS server to perform 802.1X using the recommended EAP method PEAP + MSCHAPV2.

2 Set up each WSS as a RADIUS client.

3 Define any desired Nortel vendor-specific attributes (VSAs) in the RADIUS server's dictionary.

The vendor-specific attributes (VSAs) created by Nortel are embedded according to the procedure recommended in RFC 2865, with Vendor-ID set to 562. Table 2 describes the Nortel VSAs, listed in order by vendor type number.

Table 2: Nortel VSAs

Attribute	Type, Vendor ID, Vendor Type	Rcv in Access Resp?	Sent in Access Reqst?	Sent in Acct Reqst?	Description
VLAN-Name	3, 562, 231	Yes	No	Yes	Name of the VLAN to which the client belongs.
Mobility-Profile	3, 562, 232	Yes	No	No	Name of the Mobility Profile used by the authorized client.
Encryption-Type	3, 562, 233	Yes	No	No	Type of encryption used to authenticate the client.
Time-Of-Day	3, 562, 234	Yes	No	No	Day(s) and time(s) during which a user can log into the network.
SSID	3, 562, 235	Yes	No	Yes	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to Nortel radios in the Mobility Domain.
End-Date	3, 562, 236	Yes	No	No	Date and time after which the user is no longer allowed to be on the network. Use the following format: YY/MM/DD-HH:MM
Start-Date	3, 562, 237	Yes	No	No	Date and time at which the user becomes eligible to access the network. Use the following format: YY/MM/DD-HH:MM
URL	3, 562, 238	Yes	No	No	URL to which the user is redirected after successful Web authentication. Use the following format: http://www.example.com

4 Configure each user record with authorization rules (username and password) and with either the Vlan-Name attribute (Nortel VSA) or the RADIUS Tunnel-Private-Group-ID to assign users to VLANs.

Other attributes are optional.

Create a Service Profile for 802.1X Access

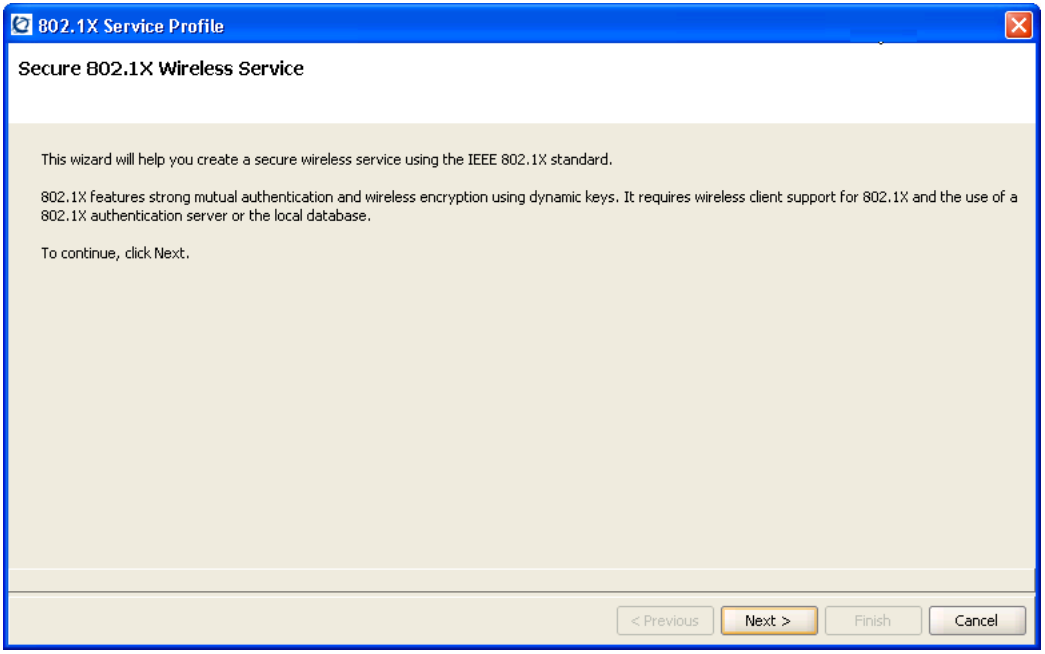
A service profile contains the configuration for the service you want to offer, such as employee access, guest access, or VoWIP.

For more information about service profiles, refer to "Wireless Configuration" on page 40. For more information about service sets, refer to "Which Services to Provide?" on page 35.

To create an 802.1X service profile

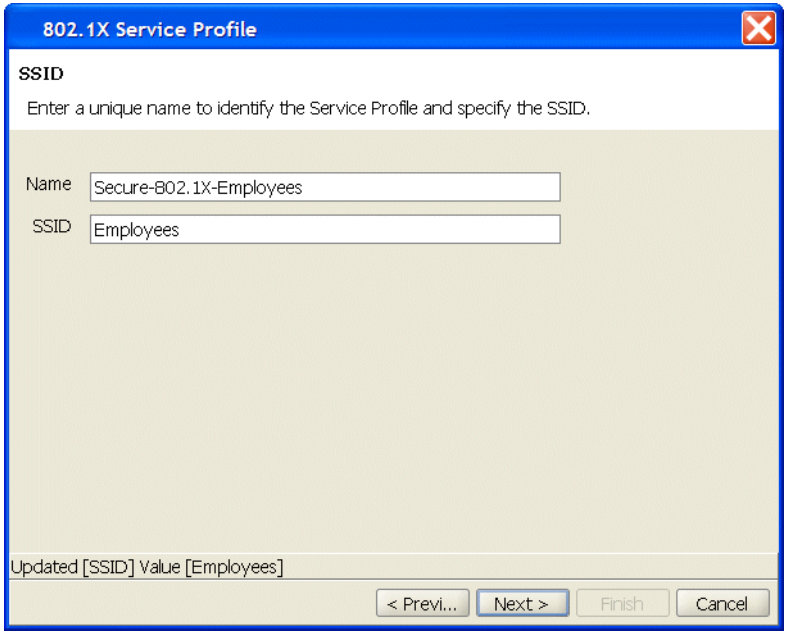
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand Wireless, then select Wireless Services.
4. In the Task List panel, select 802.1X Service Profile.

   The 802.1X Service Profile wizard appears.


802.1X Service Profile
Secure 802.1X Wireless Service
This wizard will help you create a secure wireless service using the IEEE 802.1X standard.
802.1X features strong mutual authentication and wireless encryption using dynamic keys. It requires wireless client support for 802.1X and the use of a 802.1X authentication server or the local database.
To continue, click Next.
< Previous
Next >
Finish
Cancel

5. Click **Next**.

6 Change the service profile name to *Secure-802.1X-Employees*, and use the same name for the SSID.

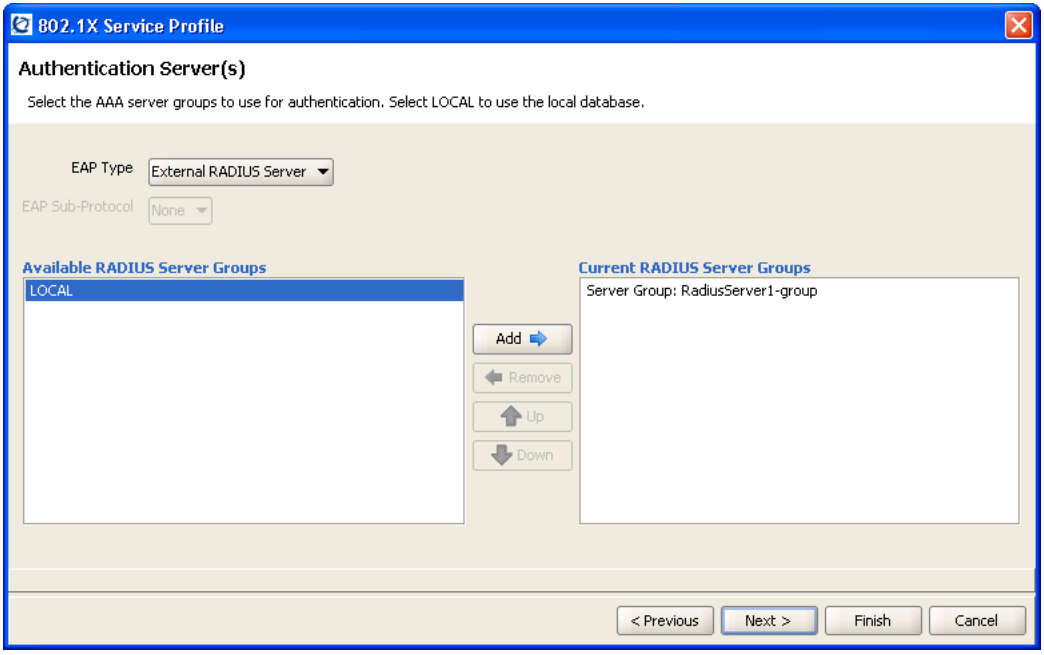


7 Click **Next**. Select WPA and deselect Dynamic WEP.

8 Click **Next**. TKIP is already selected.

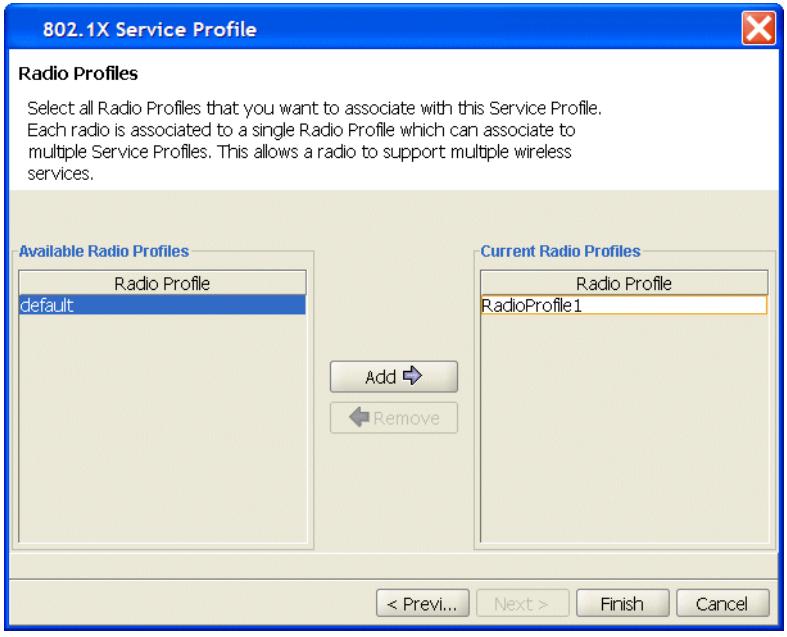
9 Click **Next**. Leave External RADIUS Server selected as the EAP Type.

10 Select the RADIUS server group in the Available RADIUS Server Groups list and click **Add**.



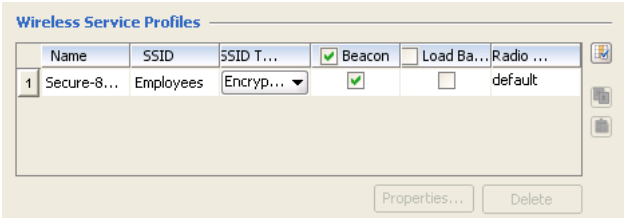
11 Click **Next**. The default VLAN screen appears. Select *vlan-mkt* in the Available Service Profiles list.

12 Click **Next**. Select *RadioProfile1* in the Available Radio Profiles list and click **Add**. Select *default* in the Current Radio Profiles list and click **Remove**.


802.1X Service Profile
Radio Profiles
Select all Radio Profiles that you want to associate with this Service Profile. Each radio is associated to a single Radio Profile which can associate to multiple Service Profiles. This allows a radio to support multiple wireless services.
Available Radio Profiles
Radio Profile
default
Add
Remove
Current Radio Profiles
Radio Profile
RadioProfile1
< Previ...
Next >
Finish
Cancel

13 Click **Finish**.

The new service profile appears in the Content panel.



View the Service Profile's Access Rules

Every service profile requires access rules. The access rules specify the usernames or MAC addresses that are allowed to access the SSID. The service profile wizards automatically create access rules that match on all usernames or, for VoWIP services, that match on all MAC addresses.

To view an 802.1X service profile's access rules

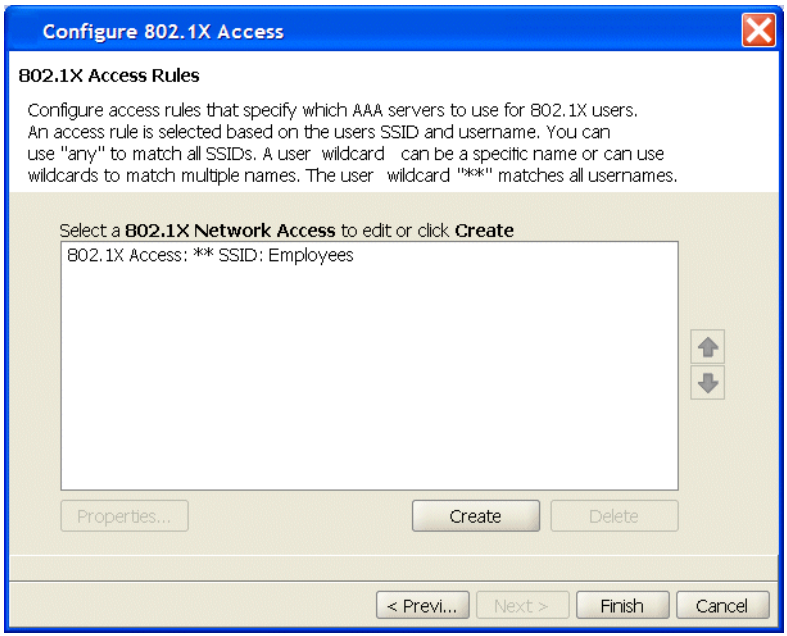
1 Select the service profile in the Wireless Service Profiles table (located in the Content panel).

A Setup group appears in the Task List panel.

2 In the Task List panel, select 802.1X Access.

The Configure 802.1X Access wizard appears. The wizard displays the encryption settings, access rules, and AAA settings for the service profile and allows you to change them. You also can configure new access rules using the wizard.

3 Click **Next** to page through the wizard until the 802.1X Access Rules page appears.


Configure 802.1X Access
802.1X Access Rules
Configure access rules that specify which AAA servers to use for 802.1X users.
An access rule is selected based on the users SSID and username. You can
use "any" to match all SSIDs. A user wildcard can be a specific name or can use
wildcards to match multiple names. The user wildcard "**" matches all usernames.
Select a 802.1X Network Access to edit or click Create
802.1X Access: ** SSID: Employees
Properties...
Create
Delete
< Previ...
Next >
Finish
Cancel

The 802.1X Access Rules page lists the access rules configured for the service profile. The userglob and SSID name are show. The userglob can be a specific username, part of a username with a wildcard character (*), or two wildcard characters (**) to match on all usernames.

The 802.1X Service Profile wizards uses the ** userglob in the access rule. You can use this rule, modify it, or delete it and create a new one. You can also create additional rules. For syntax information, refer to "Wireless Service Parameters" in "Configuring Wireless Parameters" of the *Nortel WLAN Management Software 2300 Series Reference Guide*.

To modify or create access rules

Refer to "Modifying SSID Encryption Settings and Access Rules" in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

Set Up VLANs on WSSs

WSSs in a Mobility Domain contain a user's traffic within the VLAN to which the user is assigned. For example, if you assign a user to VLAN red, the WSSs in the Mobility Domain contain the user's traffic within VLAN red configured on the switches. The VLANs you configure for service sets support wireless users—they do not serve as management VLANs.

If a WSS is connected to the network by only one IP subnet, the WSS must have at least one VLAN configured. Optionally, each VLAN can have its own IP address. However, no two IP addresses on the switch can belong to the same IP subnet. Define user VLANs on at least one WSS within the Mobility Domain.

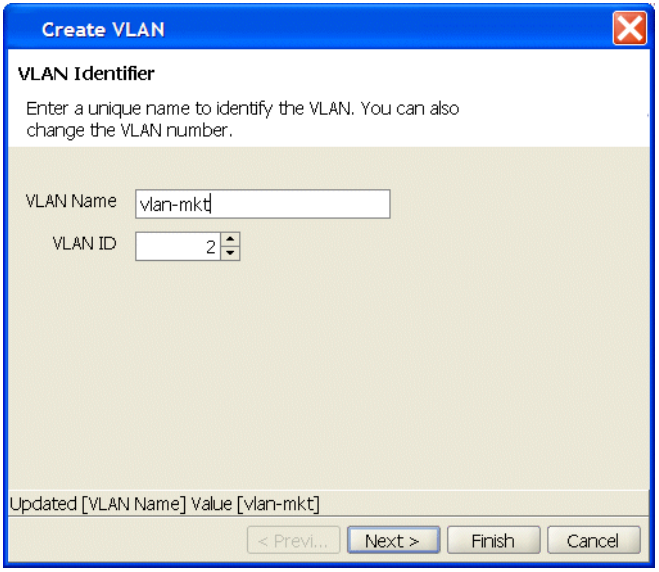
You can configure the Spanning Tree Protocol (STP) on a VLAN. STP is used to maintain a loop-free network; meaning, devices will recognize a loop in the topology and block one or more redundant paths, creating a loop-free path.

The WLAN 2300 System Software (**WSS Software**) supports Per-VLAN Spanning Tree protocol (PVST). PVST allows a separate spanning tree in each VLAN. STP is disabled by default on all VLANs, but it is configurable for individual VLANs. STP does not run on AP ports or wired authentication ports and does not affect traffic flow on these port types.

To set up a VLAN on a WSS

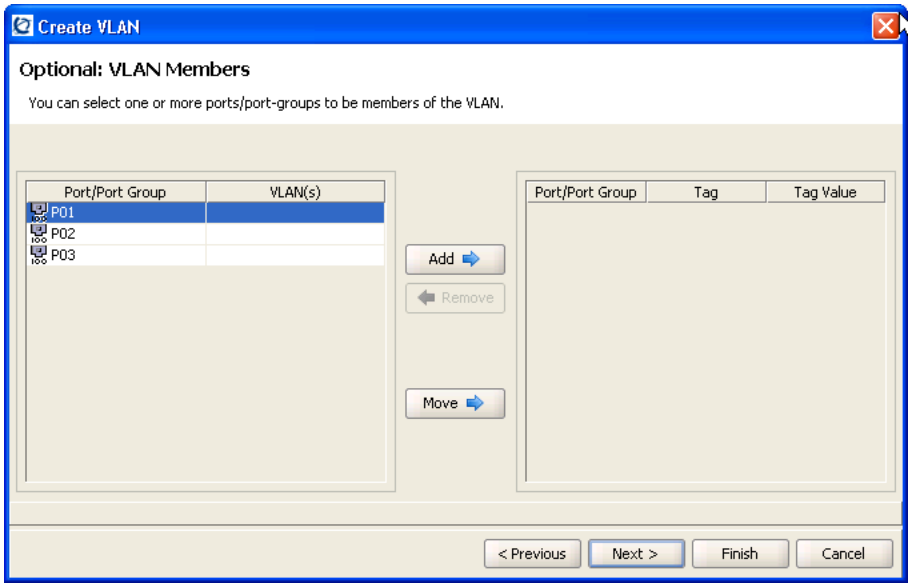
1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand System, then select VLANs.
4. In the Task List panel, select VLAN.

   The Create VLAN wizard appears.



5. Enter *vlan-mkt* as the VLAN name and use the VLAN ID suggested by the wizard.

6 Click **Next**. The VLAN Members window appears. Select the ports you want to use in the VLAN and click **Add** or **Move**.



- **The Add button adds the ports to the new VLAN without removing them from any other VLANs.**
- **The Move button removes the ports from all other VLANs, and places them in the new VLAN.**

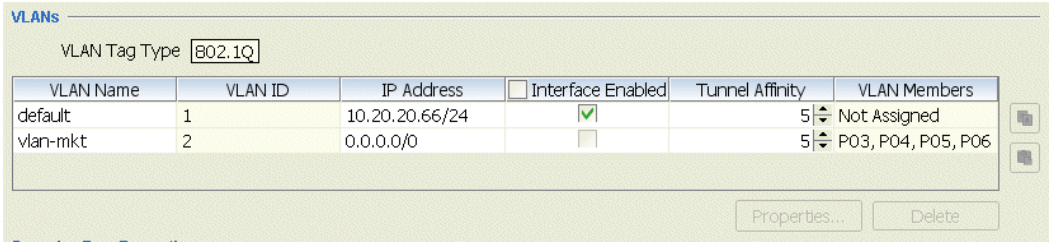
The ports appear in the Current Members list.

To tag ports in the VLAN, select Tag and edit the tag value. (Tagging is required if you click **Add**, because the ports are then members of multiple VLANs.)

7 Click **Next**. (Optional) To assign an IP interface to the VLAN, edit the IP address or select DHCP Client. To enable the IP interface, select Interface Enabled.

8 Click **Finish**.

The new VLAN appears in the Content panel.



What's Next?

After creating Employee services, create additional services.

For information about configuring additional services, refer to the following:

- "Configure Guest Access Services" on page 69
- "Configure Voice over Wireless IP Service" on page 85

After creating additional services, create your RF environment, deploy the configuration, and enable monitoring.

For information about creating ~~your~~ the RF environment, refer to the following:

- "Using Auto-RF" on page 101
- "Using Auto-RF with Modelling" on page 109
- "Using RF Planning" on page 129

For information about deploying the configuration and enabling network monitoring, refer to "Managing and Monitoring Your Network" on page 161.

Configure Guest Access Services

Guest Access is access for visitors at your location and is typically clear (no encryption).

This section contains the following information about how to configure Guest access services:

- "Task Table" on page 70
- "Step Summary" on page 72
- "Optional: Configure Mobility Profiles" on page 84

Table 3 on page 70 contains the tasks to configure Guest access services. The "Step Summary" provides the configurable options to set. The table contains references to-"Example: Configure Employee Access" on page 56. The references are provided in case you want to refer to detailed steps. However, be sure to use the configurable options for Guest Access services set forth in the "Step Summary" on page 72. Optionally, you can configure mobility profiles for your Guest Access services to limit access based on criteria, such as RF coverage area or time of day.

Task Table

Table 3 contains the tasks you need to perform to create Guest access services. For a summary of configurable items, refer to "Step Summary" on page 72.

Table 3: Creating a Service for Guest Access

Task	Path	Primary Parameters to Configure
"Create a Radio Profile" on page 57	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click Radio Profiles. 5. Select Radio Profile in the Task List.	From the Create Radio Profile wizard: • Radio profile name: Enter a name After you create the service profile, you can map it to the radio profile. After you install the APs, you can map their radios to the radio profile. **Note:** The examples in this chapter configure the radio profile first. However, you also can configure the radio profile later as part of service profile configuration.
"Create a User Group and Guest Users" on page 73	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand AAA. 4. Click Local User Database. 5. Select User in the Task List.	From the Create Named User wizard: • Username: Enter name • Password: Enter password • Authorization attributes: Configure the end-date, to specify when the account expires
"Create a Service Profile for Guest Access with Web Login" on page 76	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click Wireless Services. 5. Select Web Portal Service Profile in the Task List.	From the Create Service Profile wizard: • Service profile name: Edit name • SSID name: Enter name • SSID Type: Use Clear (unencrypted) • VLAN Name: Enter name • Authentication server: Select LOCAL or a RADIUS server group • Radio profile: Select one

Table 3: Creating a Service for Guest Access (continued)

Task	Path	Primary Parameters to Configure
"Set Up VLANs on WSSs" on page 66	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand System. 4. Click VLANs. 5. Select VLAN in the Task List.	From the Create VLAN wizard: • VLAN Name: Enter name • VLAN ID: Select number • IP Address: Enter IP Address • Ports: Select ports and either move (use only in the new VLAN) or add them (share with other VLANs) • If you add ports, select Tag
"Optional: Configure Mobility Profiles" on page 84	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand AAA. 4. Click Mobility Profiles. 5. Select Mobility Profile in the Task List.	From the Create Mobility Profile wizard: • Profile Name: Enter one • Ports: Use Selected • Select the ports or Distributed APs

Step Summary

The following list summarizes the fields selected or configuration items entered to configure Guest access.

1. Create a radio profile.
   - **From the Radio Profile wizard, enter *RadioProfile1* as the name of the radio profile.**
   - **Click Finish.**
2. Configure users in the local database:
   - **From the Create Named User wizard, enter *guest1* as username and *guest1pass* as the password.**
   - **Configure the end-date authorization attribute to specify when the account expires.**
   - **Allow the wizard to create a server group or select a configured server group.**
   - **Click Finish.**
3. Create a Web-Portal service profile.
   - **From the Web-Portal Service Profile wizard, click Next and enter *Web-Portal-Guests* as the Name of the service profile and *Guests* as the SSID.**
   - **Click Next. Enter *guest_vlan*.**
   - **Click Next. Click Next again. Select LOCAL and click Add.**
   - **Click Next. Click Next again. Select *RadioProfile1* and click Add. Select *default* and click Remove.**
   - **Click Finish.**
4. Set up a VLAN on the WSSs.
   - **From the Create VLAN wizard, enter *guest-vlan* as the VLAN name.**
   - **Click Next. Select the VLAN ports. Click Add to share them with other VLANs or Move to use them exclusively in this VLAN. If you click Move, then select Tag.**
   - **Click Finish.**
5. Optional: Configure a Mobility Profile.
   - **From the Create Mobility Profile wizard, enter the Profile Name.**
   - **Choose "Selected".**
   - **Choose the Ports or Distributed APs to which you'll restrict guest users to certain geographic areas of your network.**
   - **Click Finish.**

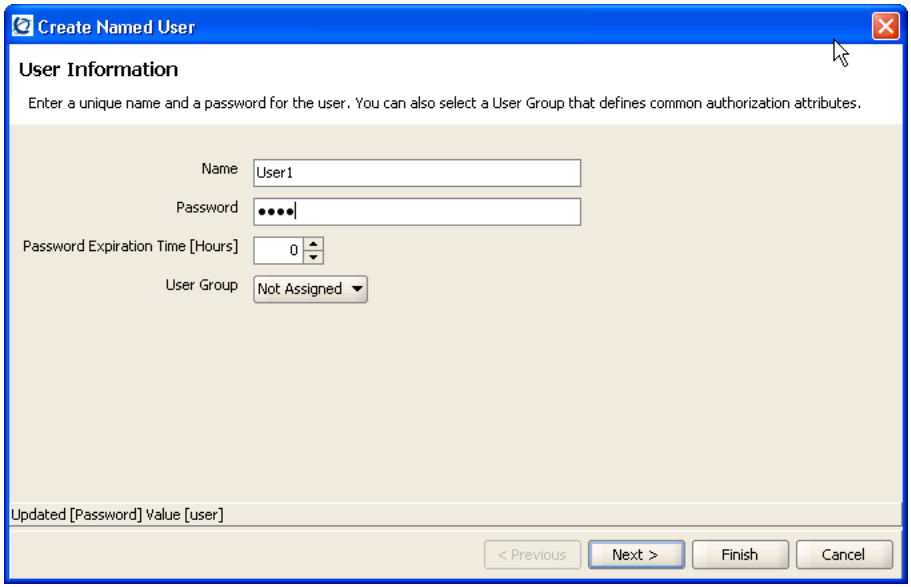
For detailed information about the steps, refer to the "Task Table" on page 70. New configuration items that were not part of the "Configure Employee Access Services" on page 54 example are included in the following sections.

Create a User Group and Guest Users

One way to administer guest user accounts is to configure a guest user group and add users to the group.

To create users

1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand AAA, then select Local User Database.
4. In the Task List panel, select Create User.



5. Type the username and password.

   Leave the User Group unassigned. (You can add the user to the group when you create the group.)

   Enter Password Expiration Time in hours.

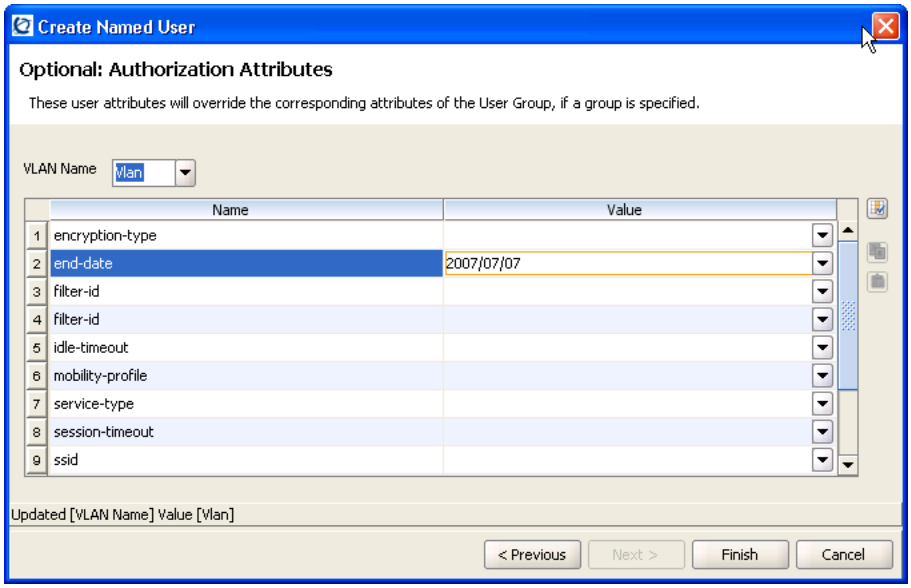
Note. For Web Portal access, specify the VLAN name when you configure the guest service profile. (See step 8 on page 78.)

6. Click **Next**.

   The wizard lists the following authorization attributes you can configure for the user. A very useful authorization attribute for guest users is the end-date, which specifies the date and time when the user's network access expires.

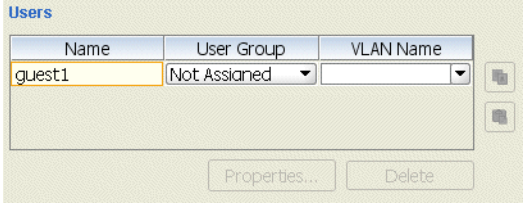
7 Click in the Value column next to end-date and specify the ending date and time for this user's guest access. Use the following format:

YY/MM/DD-HH:MM



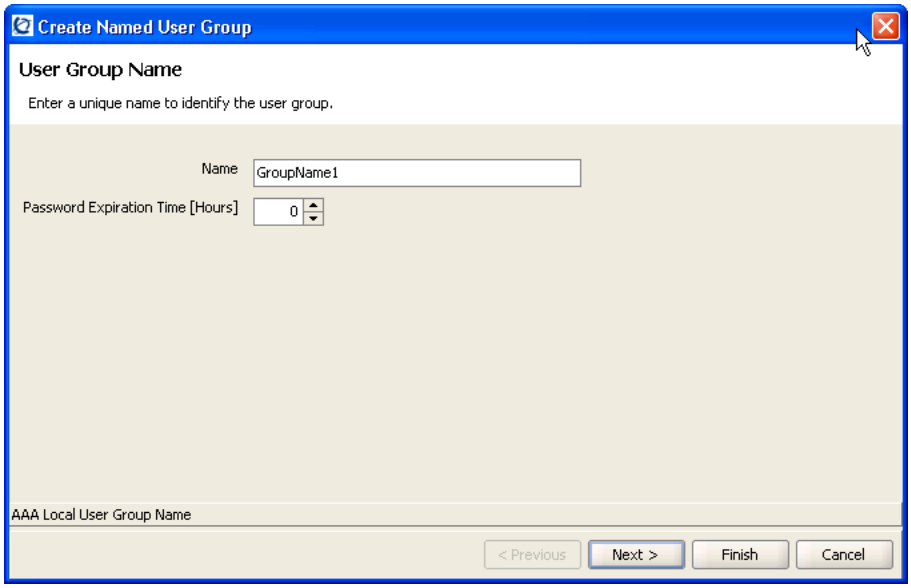
8 Click **Finish**.

The new user appears in the Content panel.



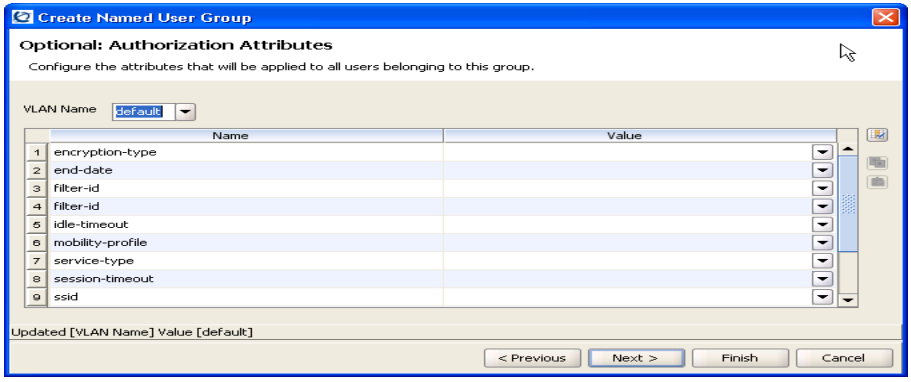
To create a user group and add users to the group

1 In the Task List panel, select User Group.



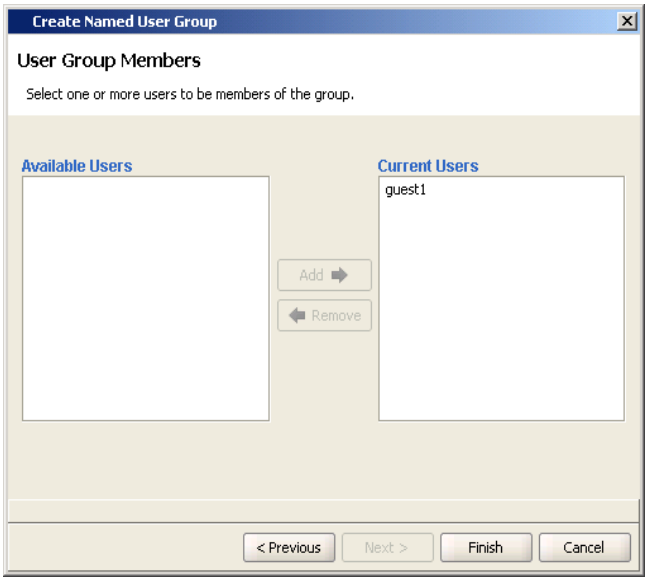
2 Type a name for the group in the name box and enter the password expiration time in the Password Expiration Time box and then click **Next**.

The wizard lists the authorization attributes you can configure for the group. For this example, leave the attributes unconfigured.



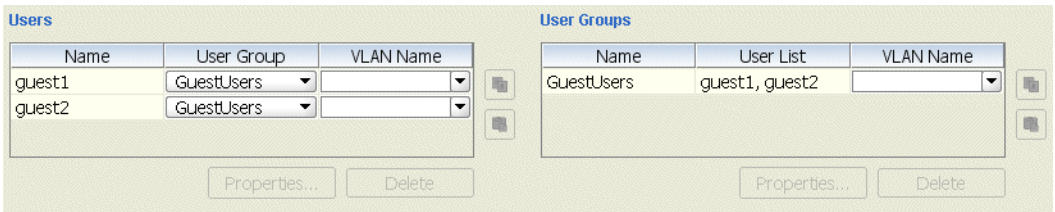
Note. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user.

3 Click **Next**. The users configured in the local database are listed. Select the guest users in the Available Users list and click **Add**.



4 Click **Finish**.

The new group appears in the Content panel.



Create a Service Profile for Guest Access with Web Login

To create a Web-Portal service profile

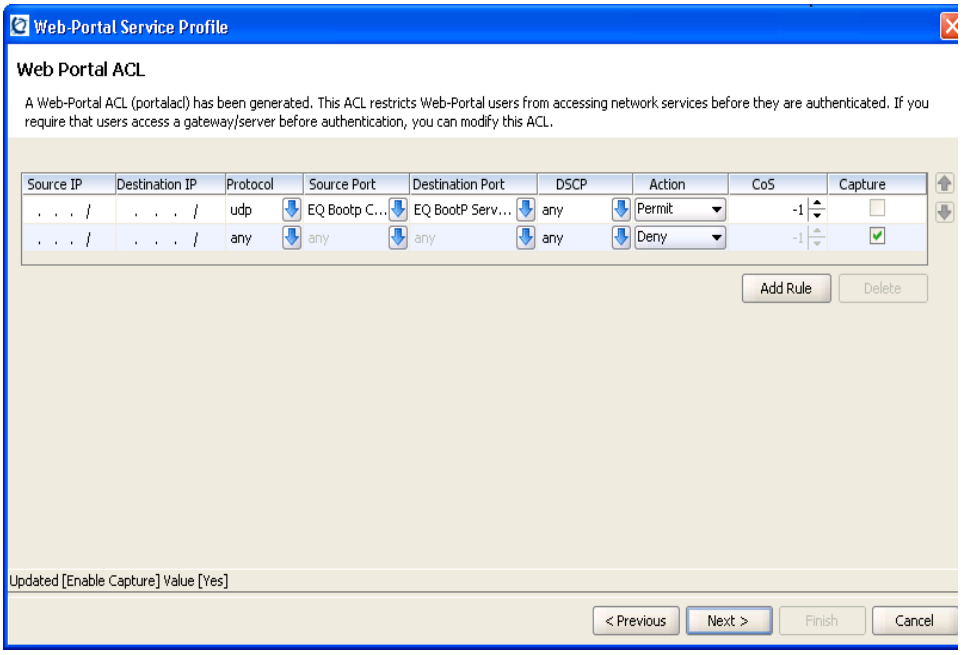
1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand Wireless, then select Wireless Services.

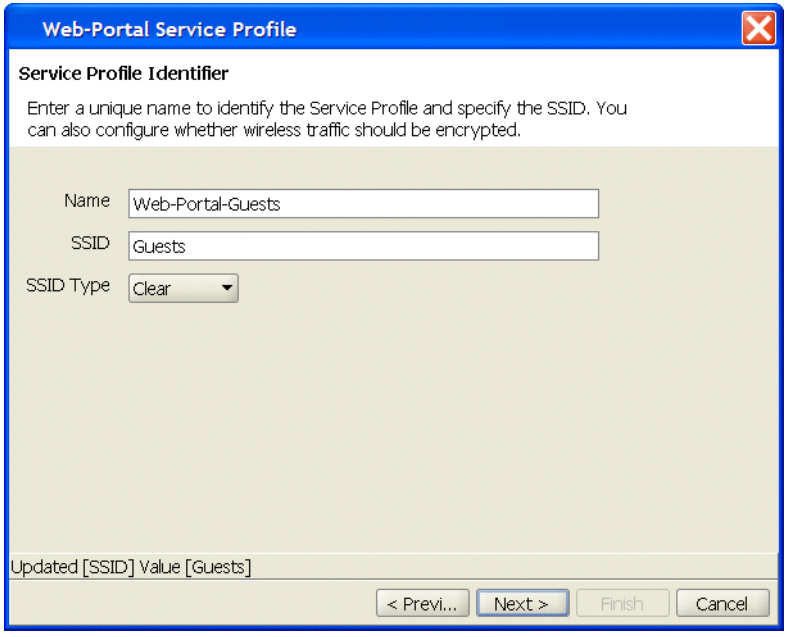
4 In the Task List panel, select Web-Portal Service Profile.

The Web-Portal Service Profile wizard is displayed.



5 Click **Next**.

6 Change the service profile name to *Web-Portal-Guests*, and use the name *Guests* for the SSID.



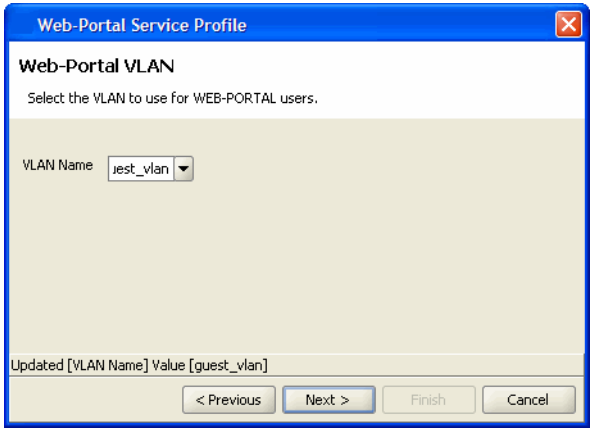
7 Select one of the following SSID types:

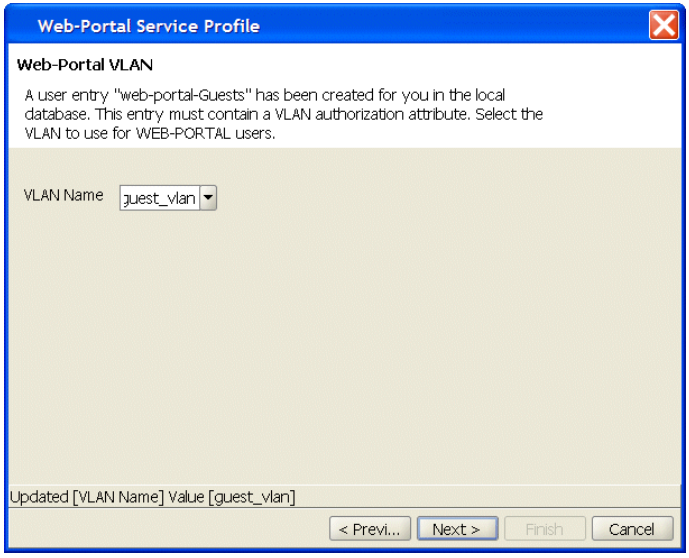
- **Encrypted—Traffic on the SSID is encrypted.**
- **Clear—Traffic on the SSID is unencrypted.**

For this example, Clear is selected.

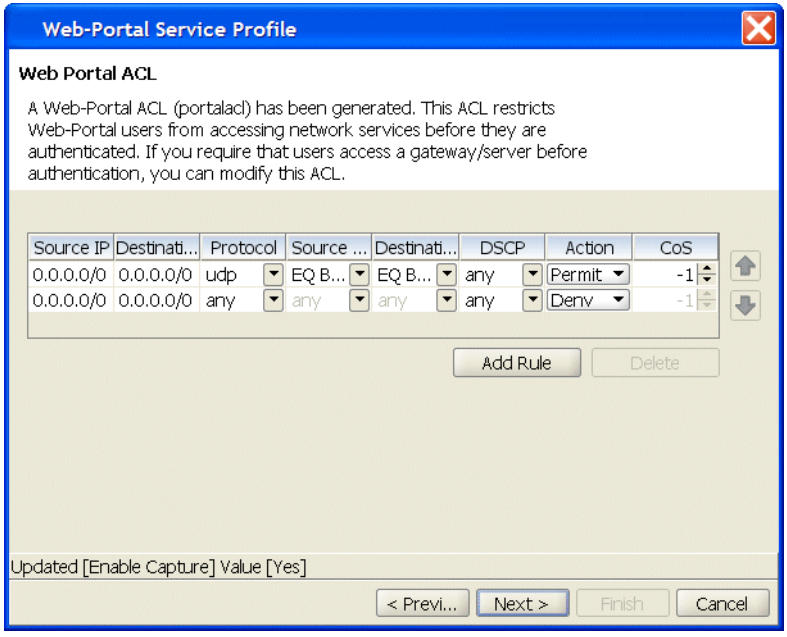
8 Click **Next**. Type or select the name of the VLAN you want to place your guest users in. For this example, use *guest_vlan*.

Note. Typing the VLAN name here does not actually configure the VLAN. To configure a VLAN, refer to "Set Up VLANs on WSSs" on page 66.




Web-Portal Service Profile
Web-Portal VLAN
A user entry "web-portal-Guests" has been created for you in the local database. This entry must contain a VLAN authorization attribute. Select the VLAN to use for WEB-PORTAL users.
VLAN Name
guest_vlan
Updated [VLAN Name] Value [guest_vlan]
< Previ...
Next >
Finish
Cancel

9 Click **Next**. The wizard displays the ACL that will automatically be added to the configuration. The ACL restricts users to DHCP traffic only while the users are in the portal and are being authenticated. After successful authentication, the user is allowed through the portal and the ACL no longer applies to the user session.

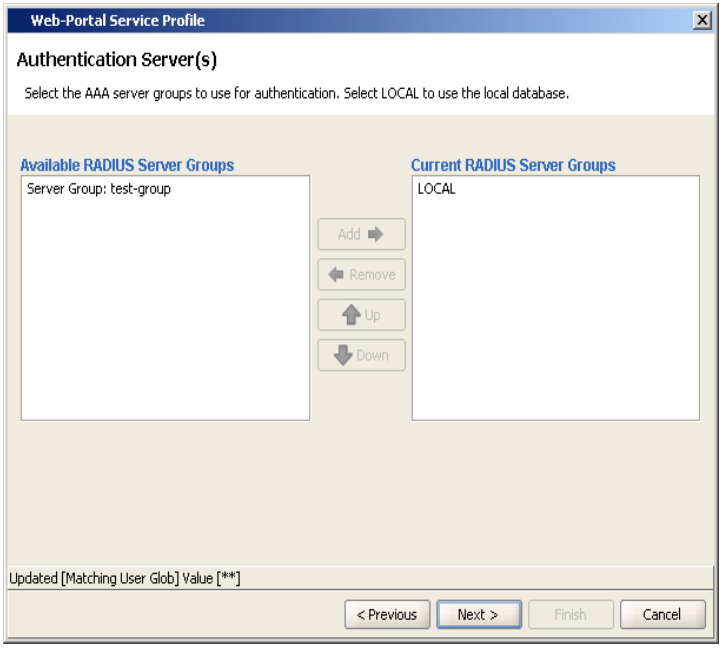


10 Click **Next**. Select the location of the user information and click **Add**.

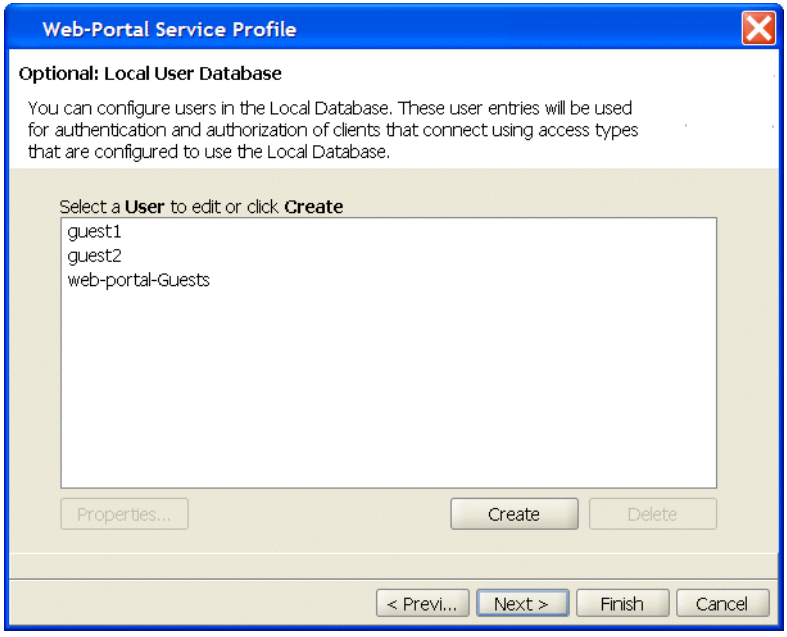
- **LOCAL—The switch's local database**
- **RADIUS server group—group of external RADIUS servers**

  (For a server group to be available in the wizard, the group must already be configured. Refer to "Configure RADIUS Servers" on page 58.)

For this example, LOCAL is selected.



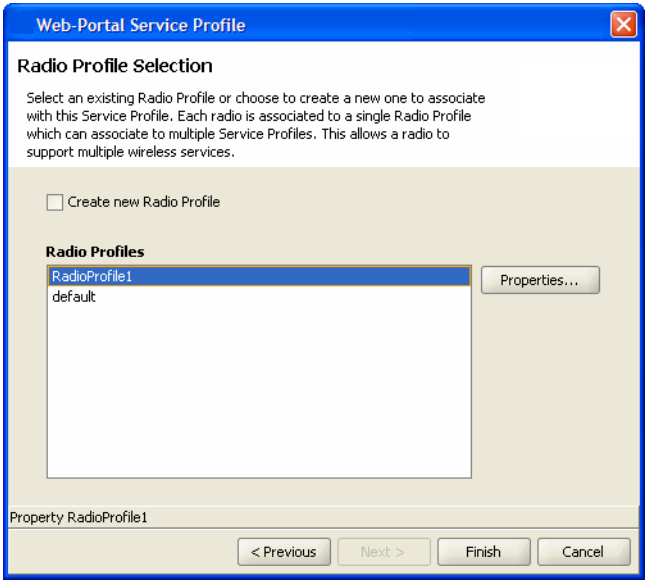
11 Click **Next**. The wizard shows the user names configured in the local database.

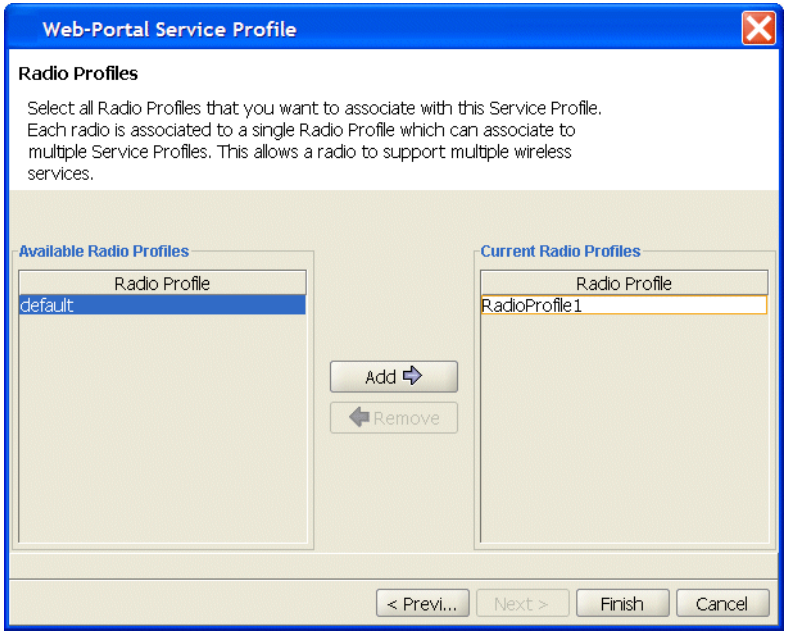

Web-Portal Service Profile
Optional: Local User Database
You can configure users in the Local Database. These user entries will be used for authentication and authorization of clients that connect using access types that are configured to use the Local Database.
Select a User to edit or click Create
guest1
guest2
web-portal-Guests
Properties...
Create
Delete
< Previ...
Next >
Finish
Cancel

The users created in "To create users" on page 73 are listed.

If you need to add users, click **Create** in the wizard.

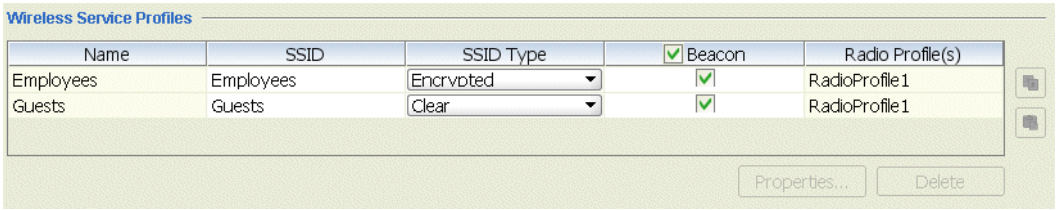
12 Click **Next**. Select *RadioProfile1* in the Available Radio Profiles list and click **Add**. Select the default radio profile and click **Remove**.


Web-Portal Service Profile
Radio Profile Selection
Select an existing Radio Profile or choose to create a new one to associate with this Service Profile. Each radio is associated to a single Radio Profile which can associate to multiple Service Profiles. This allows a radio to support multiple wireless services.
Create new Radio Profile
Radio Profiles
RadioProfile1
default
Properties...
Property RadioProfile1
< Previous
Next >
Finish
Cancel


Web-Portal Service Profile
Radio Profiles
Select all Radio Profiles that you want to associate with this Service Profile. Each radio is associated to a single Radio Profile which can associate to multiple Service Profiles. This allows a radio to support multiple wireless services.
Available Radio Profiles
Radio Profile
default
Add
Remove
Current Radio Profiles
Radio Profile
RadioProfile1
< Previ...
Next >
Finish
Cancel

13 Click **Finish**.

The new service profile appears in the Content panel.



View the Service Profile's Access Rules

To view a Web-Portal service profile's access rules

1. Select the service profile in the Wireless Service Profiles table (located in the Content panel).

   A Setup group appears in the Task List panel.

2. In the Task List panel, select Web Portal Access.

   The Configure Web-Portal Access wizard appears. The wizard displays the encryption settings, access rules, and AAA settings for the service profile and allows you to change them. You also can configure new access rules using the wizard.

   The wizard is similar to the 802.1X Access wizard, but shows access information for the Web-Portal service profile. (Refer to "View the Service Profile's Access Rules" on page 65.)

Optional: Configure Mobility Profiles

Mobility Profile™ attributes allow or deny access to the network for a specific user or group of users. When you create a Mobility Profile, specify which AP ports, Distributed APs, or wired authentication ports are to be included. Typically, include ports that are defined as AP ports or Distributed APs. You can specify that all or no ports are included, or you can specify a list of ports to be included.

When you apply the Mobility Profile, guests have access only through specific areas of your WLAN—if they roam outside of a designated area supported by a WSS or certain APs, they no longer have access to the Internet.

After creating a Mobility Profile, assign that profile to users created in the local WSS user database or users who are authenticated and authorized by a RADIUS server. To assign the profile to users in the WSS user database, add the Mobility Profile name when creating or modifying a user or user group. To add the profile on a RADIUS server, assign the name of the Mobility Profile by using the Mobility-Profile RADIUS attribute, which is a Nortel vendor-specific attribute (VSA).

To create a Mobility Profile

1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand AAA, then select Mobility Profiles.
4. In the Task List panel, select Mobility Profile.

   The Create Mobility Profiles wizard appears.

5 In the Profile Name box, type the name of the Mobility Profile.

The name can be up to 16 alphanumeric characters, and it cannot contain tabs.

Note. The Mobility Profile Name has to be defined as an authorization attribute in the defined users or user groups in the local database.

6 In the Ports list, specify ports to include in the Mobility Profile.

- **All—Include all AP or wired authentication ports. Go to step 10.**
- **Selected—Include a selected list of ports. Go to step 7.**
- **None—Include no ports. Go to step 10.**

7 Select the ports to be included in the Mobility Profile and click **Add**.

8 Click **Next**. In the Distributed APs list, specify the Distributed APs to include in the Mobility Profile.

- **All—Include all Distributed APs. Go to step 10.**
- **Selected—Include a selected list of Distributed APs. Go to step 9.**
- **None—Include no Distributed APs. Go to step 10.**

9 Select the Distributed APs to be included in the Mobility Profile and click **Add**.

10 Click **Finish** to save the changes and close the wizard.

What's Next?

After you create Guest services, you can create another service.

For information about configuring an additional service, refer to the following:

- "Configure Voice over Wireless IP Service" on page 85

You can create your RF environment, and deploy your configuration and enable monitoring.

For information about creating your RF environment, refer to the following:

- "Using Auto-RF" on page 101
- "Using Auto-RF with Modelling" on page 109
- "Using RF Planning" on page 129

For information about deploying your configuration and enabling monitoring your network, refer to the following:

- "Managing and Monitoring Your Network" on page 161.

Configure Voice over Wireless IP Service

Voice over Wireless IP (VoWIP) is a new technology, merging VoIP (Voice over IP) with 802.11 wireless LANs to create a wireless telephone system. Organizations that add VoWIP to their wireless LANs can deploy and manage voice

and data over a single wireless backbone, reserving some portion of network bandwidth to support real-time voice communications.

For a VoWIP service (sometimes also referred to simply as *VoIP*, or *Voice over IP*), you can configure either local or RADIUS server authentication, and add Access Lists (ACLs) to restrict user access.

This section contains the following information about how to configure VoWIP services:

- "Task Table" on page 86
- "Step Summary" on page 87
- "Create a Service Profile for WMM VoWIP Devices" on page 89
- "Create a Service Profile for SVP VoWIP Devices" on page 93
- "Create a Service Profile for Avaya VoWIP Devices" on page 95

Table 4 contains the tasks you must perform to configure Guest access services. The table contains references to "Example: Configure Employee Access" on page 56. The references are provided in case you want to refer to detailed steps. However, be sure to use the configurable options for VoWIP access services set forth in the "Step Summary" on page 87. The "Step Summary" provides the configurable options you should set.

Task Table

Table 4 contains the tasks you need to perform to create VoWIP access services. For a summary of configurable items, refer to "Step Summary" on page 87.

Table 4: Creating a Service for VoWIP Access

Task	Path	Primary Parameters to Configure
"Create a Radio Profile" on page 57	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click Radio Profiles. 5. Select Radio Profile in the Task List.	From the Create Radio Profile wizard: • Radio profile name: Enter a name For SpectraLink, from the Radio Profile Properties dialog: • 802.11 attributes: Change DTIM to 3 After you create the service profile, you can map it to the radio profile. After you install the APs, you can map their radios to the radio profile. **Note:** The examples in this chapter configure the radio profile first. However, you also can configure the radio profile later as part of service profile configuration.

Table 4: Creating a Service for VoWIP Access (continued)

Task	Path	Primary Parameters to Configure
"Create a Service Profile for Voice" on page 89	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand Wireless. 4. Click Wireless Services. 5. Select Voice Service Profile in the Task List.	From the Create Service Profile wizard: • Service profile name: Edit name • SSID name: Enter name • SSID Type: Use Clear (unencrypted) • VLAN Name: Enter name • Authentication server: Select LOCAL • Radio profile: Select one
"Set Up a VLAN for VoWIP on WSSs" on page 99	1. Tool bar option: Select Configuration. 2. Organizer panel: Expand the WSS. 3. Expand System. 4. Click VLANs. 5. Select VLAN in the Task List.	From the Create VLAN wizard: • VLAN Name: Enter name • VLAN ID: Select number • IP Address: Enter IP Address • Ports: Select ports and move them to the voice VLAN For SpectraLink, from the VLAN Properties dialog: • IGMP: Disable **Note:** SVP requires IGMP snooping to be disabled.

Step Summary

The following list summarizes the fields selected or configuration items entered to configure VoWIP access:

1 Create a radio profile.

- **From the Radio Profile wizard, enter *RadioProfileVoic* as the Name of the radio profile.**
- **Click Finish.**
- **Select the radio profile and click Properties.**
- **Select the 802.11 Attributes and change the DTIM Period to 3.**
- **Click OK.**

2 Create a Voice service profile.

- **From the Voice Service Profile wizard, click Next and enter *Voice-WMM, Voice-SVP, Voice-Avaya*, or *Voice-Vocera* as the Name of the service profile and *WMM*, *SVP*, *Avaya*, or *Vocera* as the SSID.**
- **Select the Vendor (SpectraLink, Avaya, Vocera, or Other).**
- **Click Next. Select the access type. (The examples in this section use Open Access.)**
- **Click Next. Select the data encryption method. (The examples in this section use WPA and disable Static WEP.)**
- **Click Next. Leave TKIP enabled and click Next.**

- **Click Next. Type a passphrase from 8 to 63 characters long in the Pre-shared Key box and click Generate.**
- **Click Next. Type *voice-vlan* as the VLAN name to place voice users in.**
- **Click Next. (If the device supports WMM, select WMM.)**
- **Click Next. Select *RadioProfileVoic* in the Radio Profiles list.**
- **Click Finish.**

3 Set up a VLAN on the WSSs.

- **From the Create VLAN wizard, enter *voice-vlan* as the VLAN name.**
- **Click Next. Select the VLAN ports. Click Move to use them exclusively in this VLAN.**
- **Click Finish.**
- **Select the VLAN and click Properties.**
- **Select IGMP and deselect Enabled to disable IGMP snooping.**

Create a Radio Profile for Voice

This procedure is similar to the procedure in "Create a Radio Profile" on page 57, but has additional steps to change the delivery traffic indication map (DTIM) interval to 3.

To create a radio profile for voice service

1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand Wireless, then select Radio Profiles.

4 In the Task List panel, select Radio Profile.

The Create Radio Profiles wizard is displayed.

5 Enter the name of the radio profile (for example, *RadioProfileVoic*), then click **Next** at the bottom of the wizard.

6 If APs are already configured, select the radios to map to the radio profile, then click **Move**.

WLAN Management Software removes the radios from the radio profile they are in and places them in the new profile.

If you have not configured the APs in WLAN Management Software yet, no radios are listed. You can map the radios to the radio profile later.

7 Click **Finish** to save the changes and close the wizard.

The new radio profile appears in the Content panel.

8 If you are configuring voice service for SpectraLink devices, perform the following steps:

a Select the radio profile in the Radio Profiles table and click **Properties**.

b Click the 802.11 Attributes tab.

c In the DTIM Period box, change the value to 3.

d Click **OK**.

Create a Service Profile for Voice

The Voice Service Profile wizard tailors its options based on the vendor you select. The wizard has the following vendor options:

- SpectraLink
- Avaya
- Vocera
- Other

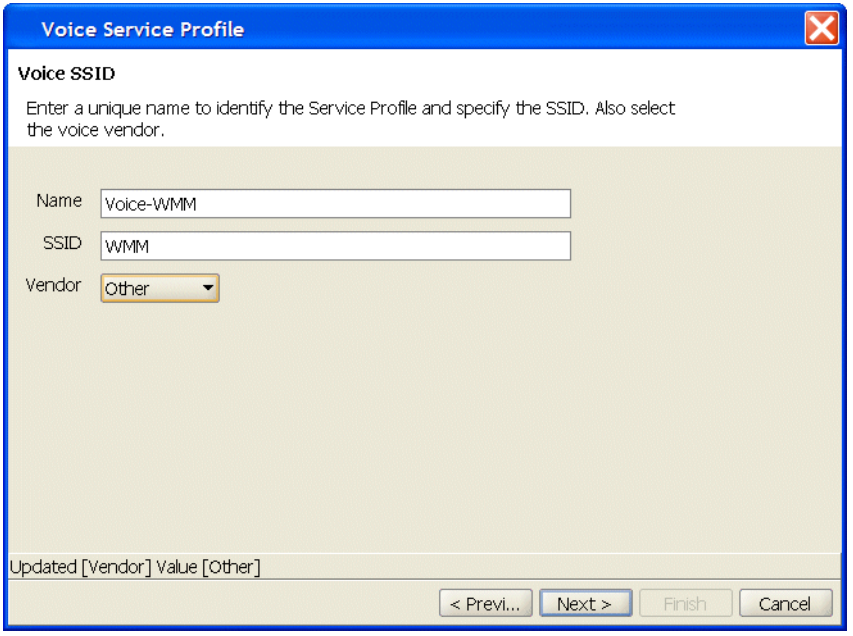
The SpectraLink, Avaya, and Vocera options configure service for proprietary VoWIP solutions from these vendors. If you are configuring VoWIP for devices that use the Wi-Fi Multimedia (WMM) standard, or a proprietary solution other than one of the listed vendors', use the Other option.

Create a Service Profile for WMM VoWIP Devices

1. Select Configuration on the toolbar.
2. In the Organizer panel, expand the WSS.
3. Expand Wireless, then select Wireless Services.
4. In the Task List panel, select Voice Service Profile.

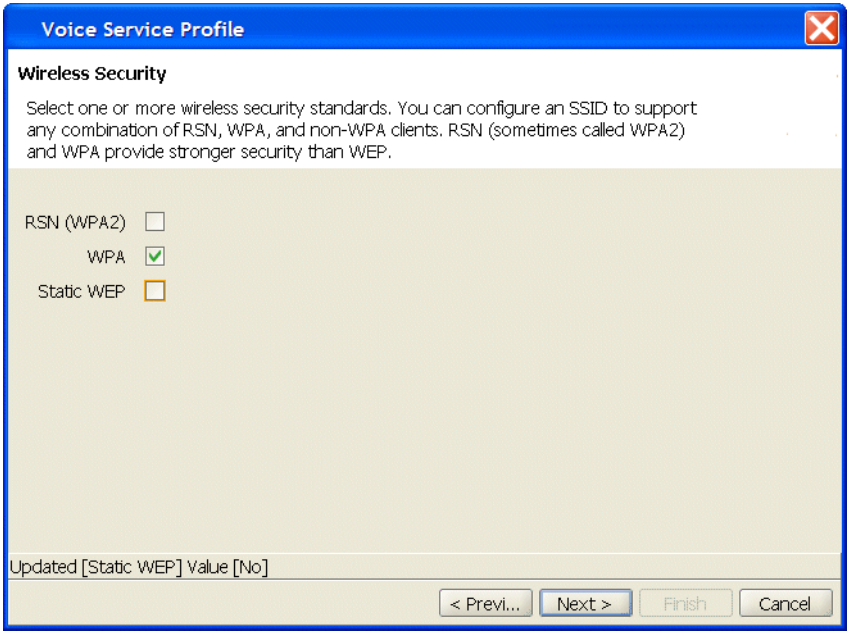
   The Voice Service Profile wizard is displayed.
5. Click **Next**.
6. Change the service profile name to *Voice-WMM*, and use the name *WMM* for the SSID.

7 Select Other from the Vendor list.

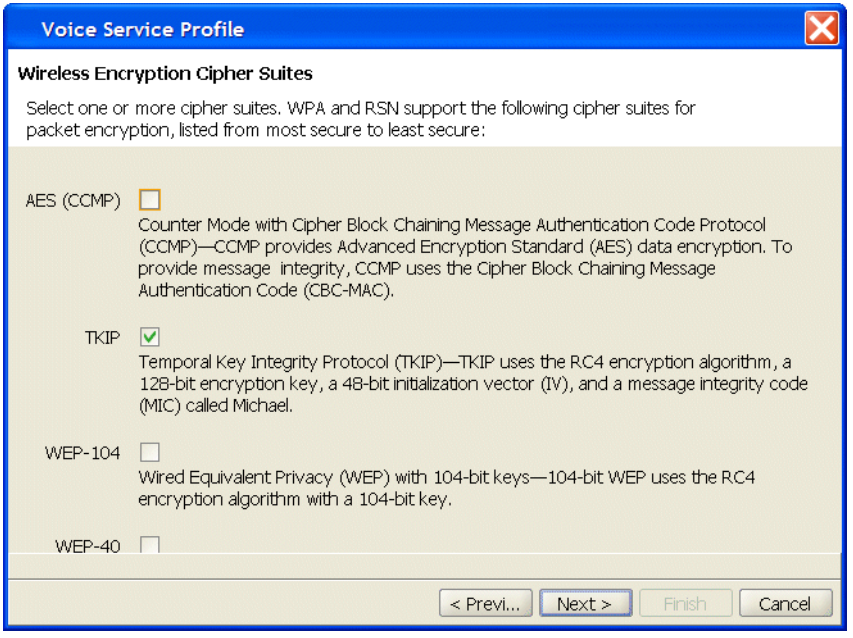


8 Click **Next**. Select Open Access and deselect MAC Access.

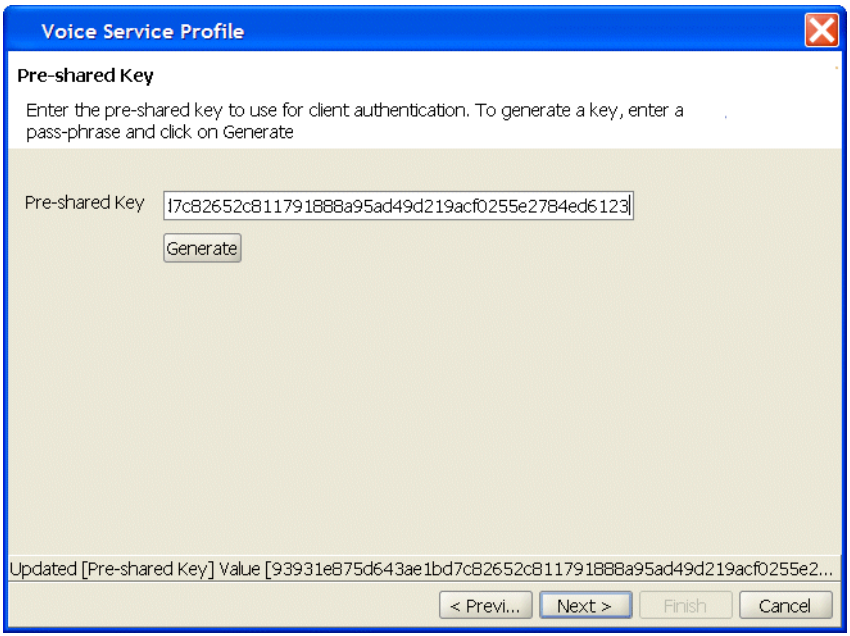
9 Click **Next**. Select WPA and deselect Static WEP.


Voice Service Profile
Wireless Security
Select one or more wireless security standards. You can configure an SSID to support any combination of RSN, WPA, and non-WPA clients. RSN (sometimes called WPA2) and WPA provide stronger security than WEP.
RSN (WPA2)
WPA
Static WEP
Updated [Static WEP] Value [No]
< Previ...
Next >
Finish
Cancel

10 Click **Next**. Leave TKIP enabled and click **Next**.


Voice Service Profile
Wireless Encryption Cipher Suites
Select one or more cipher suites. WPA and RSN support the following cipher suites for packet encryption, listed from most secure to least secure:
AES (CCMP)
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)—CCMP provides Advanced Encryption Standard (AES) data encryption. To provide message integrity, CCMP uses the Cipher Block Chaining Message Authentication Code (CBC-MAC).
TKIP
Temporal Key Integrity Protocol (TKIP)—TKIP uses the RC4 encryption algorithm, a 128-bit encryption key, a 48-bit initialization vector (IV), and a message integrity code (MIC) called Michael.
WEP-104
Wired Equivalent Privacy (WEP) with 104-bit keys—104-bit WEP uses the RC4 encryption algorithm with a 104-bit key.
WEP-40
< Previ...
Next >
Finish
Cancel

11 Click **Next**. Type a passphrase from 8 to 63 characters long in the Pre-shared Key box and click **Generate**.

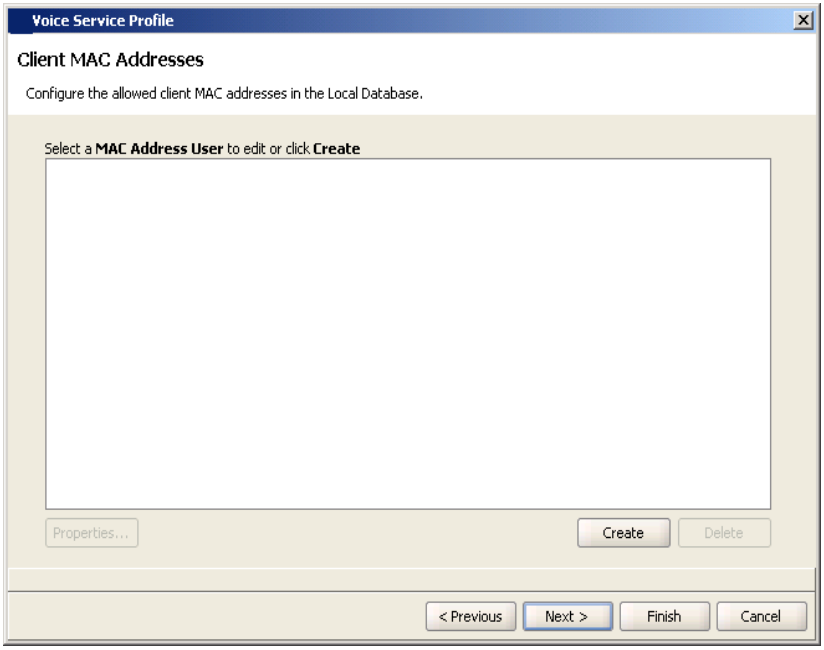

Voice Service Profile
Pre-shared Key
Enter the pre-shared key to use for client authentication. To generate a key, enter a pass-phrase and click on Generate
Pre-shared Key
!7c82652c811791888a95ad49d219acf0255e2784ed6123
Generate
Updated [Pre-shared Key] Value [93931e875d643ae1bd7c82652c811791888a95ad49d219acf0255e2...
< Previ...
Next >
Finish
Cancel

12 Click **Next**. Type or select the name of the VLAN you want to place voice users in. For this example, use *voice-vlan*.

Note. Typing the VLAN name here does not actually configure the VLAN. To configure a VLAN, refer to "Set Up VLANs on WSSs" on page 66.

13 Click **Next**. Select **Enable WMM**.

14 Click **Next**. Select a MAC Address user from the list, or click **Create** to create one. If you choose not to use a MAC Address, click **Next**.



15 Click **Next**. Select *RadioProfileVoic* in the Radio Profiles list.

16 Click **Finish**.

Create a Service Profile for SVP VoWIP Devices

1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand Wireless, then select Wireless Services.

4 In the Task List panel, select Voice Service Profile.

The Voice Service Profile wizard is displayed.

5 Click **Next**.

6 Change the service profile name to *Voice-SVP*, and use the name *SVP* for the SSID.

7 Leave SpectraLink selected in the Vendor drop-down list.

8 Click **Next**. Select Open Access and deselect MAC Access.

9 Click **Next**. Select WPA and deselect Static WEP.

10 Click **Next**. Leave TKIP enabled and click **Next**.

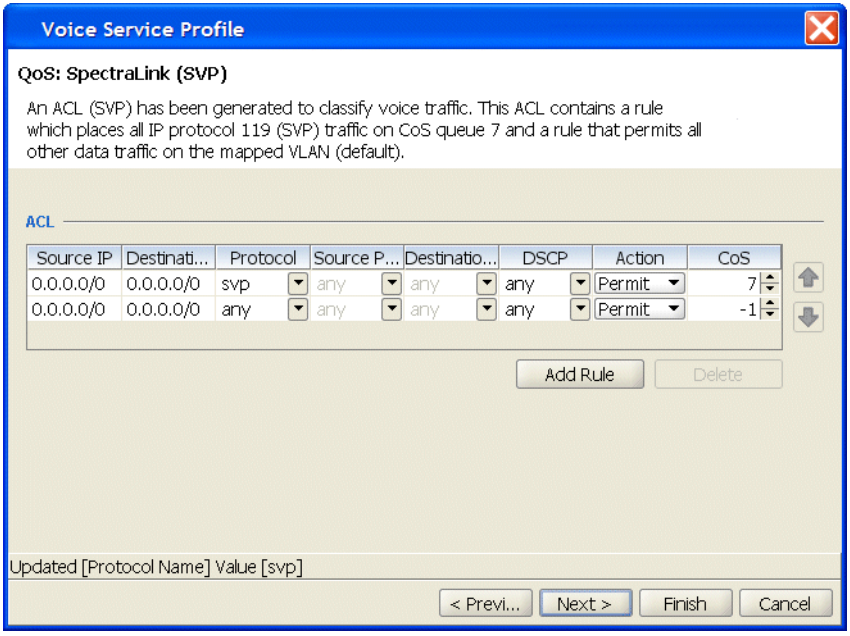
11 Click **Next**. Type a passphrase from 8 to 63 characters long in the Pre-shared Key box and click **Generate**.

12 Click **Next**. Type or select the name of the VLAN you want to place SVP users in. For this example, use *voice-vlan*.

Note. Typing the VLAN name here does not actually configure the VLAN. To configure a VLAN, refer to "Set Up VLANs on WSSs" on page 66.

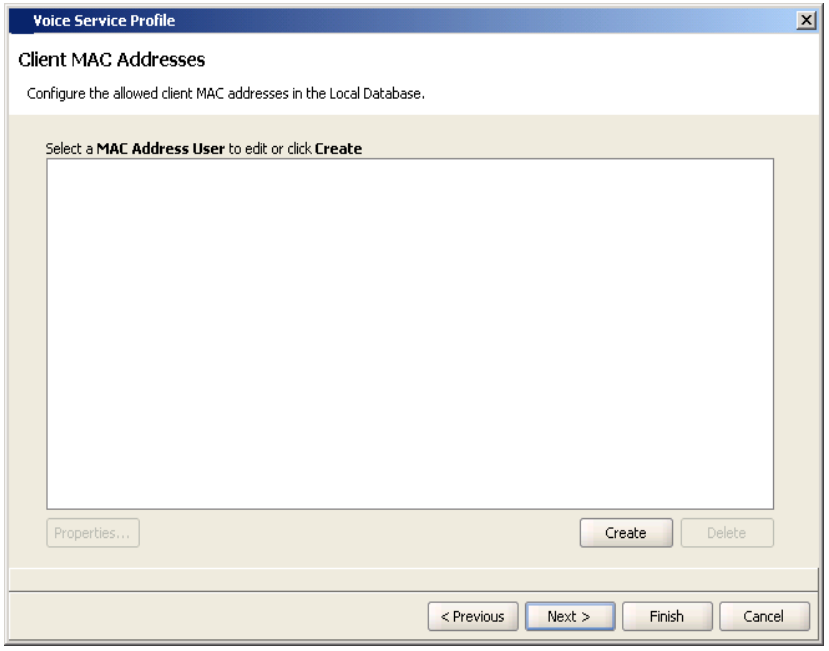
13 Click **Next**.

14 Click **Next**. The wizard displays the ACL that will automatically be added to the configuration by the wizard. The first rule in the ACL provides high -priority treatment of SVP traffic by marking IP protocol 119 (SVP) packets with CoS 7. The second rule permits all other traffic in the VLAN.



15 Click **Next**. Select *RadioProfileVoic* in the Radio Profiles list.

16 Click **Next**. Select a MAC Address user from the list, or click **Create** to create one. If you choose not to use a MAC Address, click **Finish**.



Create a Service Profile for Avaya VoWIP Devices

1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand Wireless, then select Wireless Services.

4 In the Task List panel, select Voice Service Profile.

The Voice Service Profile wizard is displayed.

5 Click **Next**.

6 Change the service profile name to *Voice-Avaya*, and use the name *Avaya* for the SSID.

7 Select Avaya in the Vendor drop-down list.

8 Click **Next**. Select Open Access and deselect MAC Access.

9 Click **Next**. Select WPA and deselect Static WEP.

10 Click **Next**. Leave TKIP enabled and click **Next**.

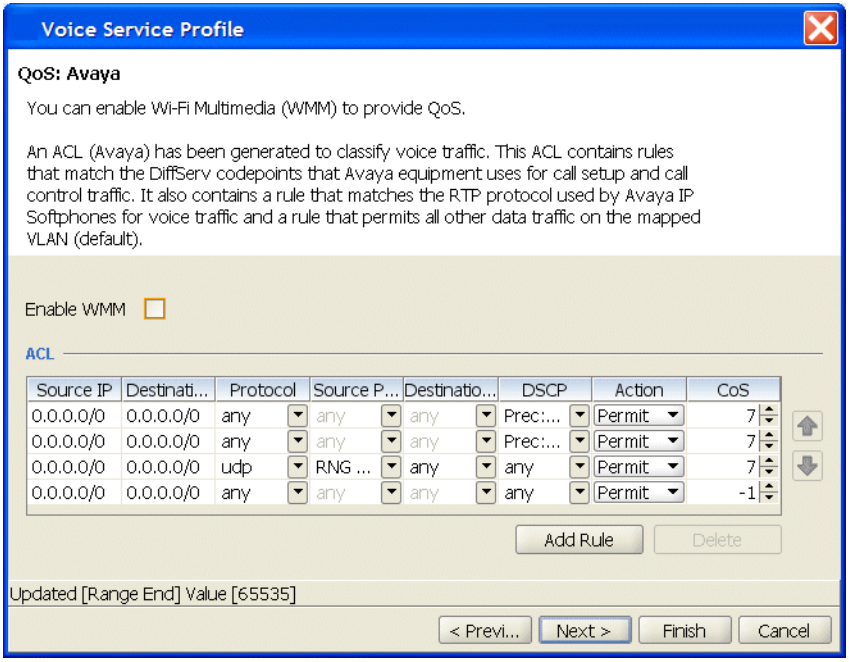
11 Click **Next**. Type a passphrase from 8 to 63 characters long in the Pre-shared Key box and click **Generate**.

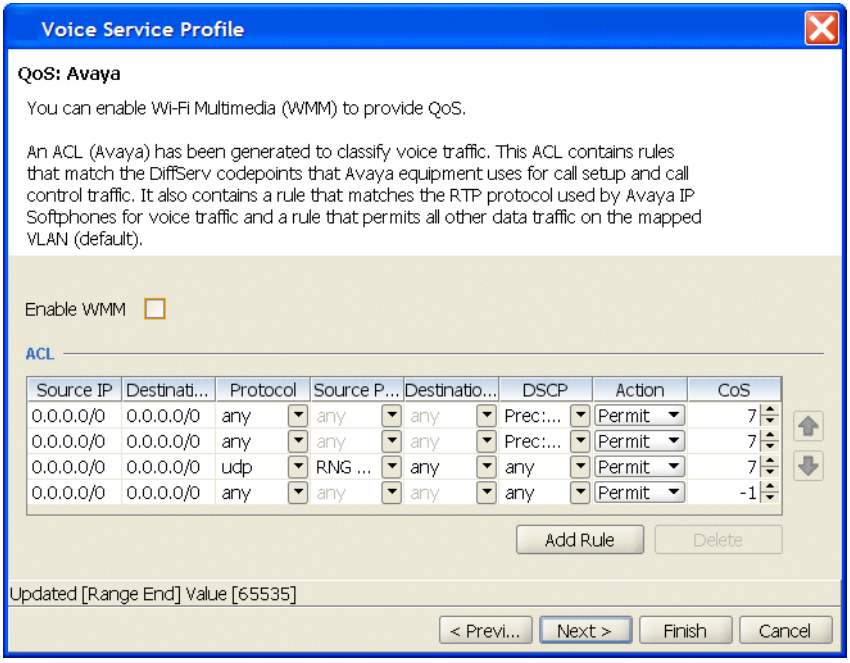
12 Click **Next**. Type or select the name of the VLAN you want to place Avaya users in. For this example, use *voice-vlan*.

Note. Typing the VLAN name here does not actually configure the VLAN. To configure a VLAN, refer to "Set Up VLANs on WSSs" on page 66.

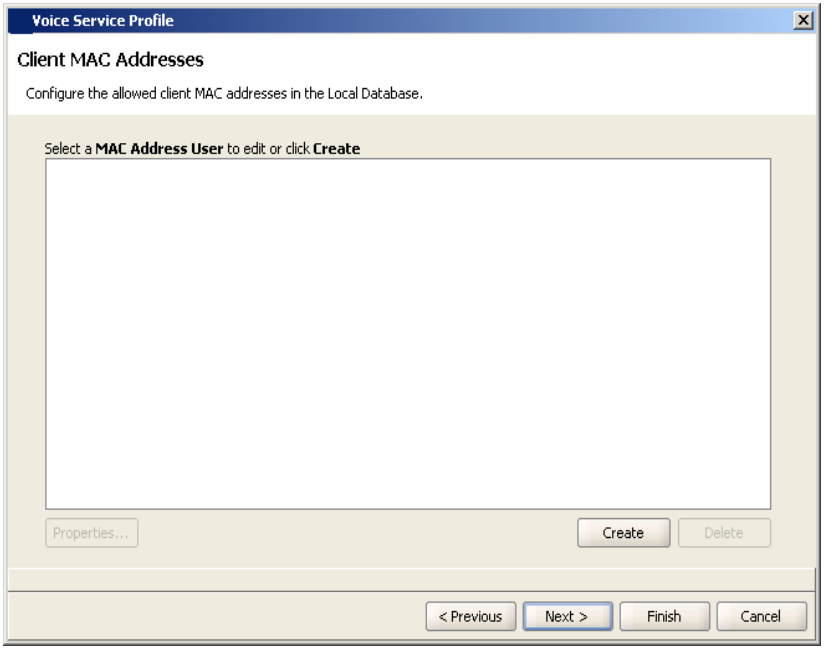
13 Click **Next**.

14 Click **Next**. The wizard displays the ACL that will automatically be added to the configuration by the wizard.


Voice Service Profile
QoS: Avaya
You can enable Wi-Fi Multimedia (WMM) to provide QoS.
An ACL (Avaya) has been generated to classify voice traffic. This ACL contains rules that match the DiffServ codepoints that Avaya equipment uses for call setup and call control traffic. It also contains a rule that matches the RTP protocol used by Avaya IP Softphones for voice traffic and a rule that permits all other data traffic on the mapped VLAN (default).
Enable WMM
ACL
Source IP
Destinati...
Protocol
Source P...
Destinatio...
DSCP
Action
CoS
0.0.0.0/0 0.0.0.0/0 any any any Prec:... Permit 7
0.0.0.0/0 0.0.0.0/0 any any any Prec:... Permit 7
0.0.0.0/0 0.0.0.0/0 udp RNG ... any any Permit 7
0.0.0.0/0 0.0.0.0/0 any any any any Permit -1
Add Rule
Delete
Updated [Range End] Value [65535]
< Previ...
Next >
Finish
Cancel


Voice Service Profile
QoS: Avaya
You can enable Wi-Fi Multimedia (WMM) to provide QoS.
An ACL (Avaya) has been generated to classify voice traffic. This ACL contains rules that match the DiffServ codepoints that Avaya equipment uses for call setup and call control traffic. It also contains a rule that matches the RTP protocol used by Avaya IP Softphones for voice traffic and a rule that permits all other data traffic on the mapped VLAN (default).
Enable WMM
ACL
Source IP
Destinati...
Protocol
Source P...
Destinatio...
DSCP
Action
CoS
0.0.0.0/0 0.0.0.0/0 any any any Prec:... Permit 7
0.0.0.0/0 0.0.0.0/0 any any any Prec:... Permit 7
0.0.0.0/0 0.0.0.0/0 udp RNG ... any any Permit 7
0.0.0.0/0 0.0.0.0/0 any any any any Permit -1
Add Rule
Delete
Updated [Range End] Value [65535]
< Previ...
Next >
Finish
Cancel

15 Click **Next**. Select a MAC Address user from the list, or click **Create** to create one. If you choose not to use a MAC Address, click **Next**.



16 Click **Next**. Select *RadioProfileVoic* in the Radio Profiles list.

17 Click **Finish**.

Create a Service Profile for Vocera VoWIP Devices

1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand Wireless, then select Wireless Services.

4 In the Task List panel, select Voice Service Profile.

The Voice Service Profile wizard is displayed.

5 Click **Next**.

6 Change the service profile name to *Voice-Vocera*, and use the name *VoceraBadges* for the SSID.

7 Select Vocera in the Vendor drop-down list.

8 Click **Next**. Leave MAC Access selected.

9 Click **Next**. Leave Static WEP selected.

10 Click **Next**.Specify the WEP keys.

- **For each key (up to four), type the key value in the corresponding key box.**

- **By default, data in unicast and multicast packets are encrypted using WEP key 1. To use another key for either type of packet, select the key number in the WEP Unicast Key Index or WEP Multicast Key Index box.**

11 Click **Next**. Type or select the name of the VLAN you want to place SVP users in. For this example, use *voice-vlan*.

Note. Typing the VLAN name here does not actually configure the VLAN. To configure a VLAN, refer to "Set Up VLANs on WSSs" on page 66.

12 Click **Create** to add MAC users to the switch's local database.

a In the User MAC Address box, type the MAC address for the user device, using colons (:) as delimiters. You must specify all 6 bytes of the MAC address.

b In the MAC User Group list, select the MAC user group that the user device belongs to, if the group is already configured.

c In the VLAN Name box, select or type the name of the VLAN that the user device belongs to (1 to 16 alphanumeric characters, with no spaces or tabs). The WSS will authorize the user for that VLAN.

d Click **Next**. In the attribute row you want to configure, click the Attribute Value column. (Refer to "Authorization Attributes" in "Configuring Authentication, Authorization, and Accounting Parameters" of the *Nortel WLAN Management Software Reference Manual*.)

e Click **Finish**.

13 Click **Next**. Select *RadioProfileVoic* in the Radio Profiles list.

14 Click **Finish**.

Set Up a VLAN for VoWIP on WSSs

This procedure is similar to the procedure in "Set Up VLANs on WSSs" on page 66, except IGMP snooping is disabled on the VLAN.

To set up a VLAN for VoWIP on a WSS

1 Select Configuration on the toolbar.

2 In the Organizer panel, expand the WSS.

3 Expand System, then select VLANs.

4 In the Task List panel, select VLAN.

The Create VLAN wizard is displayed.

5 Enter a name such as *vlan-voice* and use the VLAN ID suggested by the wizard.

6 Click **Next**. Select the ports you want to use in the VLAN and click **Add** or **Move**.

- **The Add button adds the ports to the new VLAN without removing them from any other VLANs.**
- **The Move button removes the ports from all other VLANs, and places them in the new VLAN.**

The ports appear in the Current Members list.

To tag ports in the VLAN, select Tag and edit the tag value. (Tagging is required if you click **Add**, because the ports are then members of multiple VLANs.)

7 Click **Next**. (Optional) To assign an IP interface to the VLAN, edit the IP address or select DHCP Client. To enable the IP interface, select Interface Enabled.

8 Click **Finish**.

The new VLAN appears in the Content panel.

For SVP, continue with the following steps, to disable IGMP snooping. For VoWIP types that do not require IGMP to be disabled, stop here.

9 Select the VLAN in the VLANs table and click **Properties**.

10 Click the IGMP tab.

11 Deselect Enabled, to disable IGMP snooping on the VLAN.

12 Click **OK**.

What's Next?

After you create VoWIP access services, you can create another service.

For information about configuring an additional service, refer to the following:

- "Configure Guest Access Services" on page 69

You can create your RF environment, and deploy your configuration and enable monitoring.

For information about creating your RF environment, refer to the following:

- "Using Auto-RF" on page 101
- "Using Auto-RF with Modelling" on page 109
- "Using RF Planning" on page 129

For information about deploying your configuration and enabling monitoring your network, refer to the following:

- "Managing and Monitoring Your Network" on page 161.

Using Auto-RF

What Is Auto-RF? 101
Place the Equipment 102
Configure Initial WSS Connectivity 102
Upload the WSS Configuration into a WMS Network Plan 102
Create a Service Profile 103
Create a Radio Profile and Map the Service Profile to It 104
Create Your APs 104
Apply a Radio Profile to Each Radio 107
What's Next? 108

What Is Auto-RF?

Auto-RF is a technique you can use to configure your RF (radio) network. Auto-RF is a quick method that requires minimal configuration and no RF planning or site surveys, and instead, relies on the AutoTune feature to set AP channels and power settings.

This is a great way to quickly install a WSS and APs, and observe how the network operates. The Auto-RF technique is best suited to networks containing fewer APs.

To learn more about the benefits of Auto-RF, refer to "Auto-RF" on page 37.

To use this technique:

1. Physically place the equipment (WSSs and APs) in the desired locations.
2. Configure initial WSS connectivity (configure IP addresses).
3. Upload the WSS configuration into a WMS network plan.
4. Create a service profile.
5. Create a radio profile (or use the default radio profile).
6. Map the service profile to the radio profile.
7. Create APs.
8. Apply a radio profile to each radio on an AP.
9. Deploy the configuration.

Place the Equipment

Unpack and physically install the WSSs and APs. For information about installing the equipment, refer to "Equipment Installation" on page 46.

Configure Initial WSS Connectivity

After installing a WSS, prepare it for WMS configuration and management by configuring IP connectivity between the WSS and WMS. Use the Web Quick Start (if available) or enter the **quickstart** command at the CLI prompt.

For more information about configuring initial WSS connectivity, refer to the *Nortel WLAN 2300 System Software Quick Start Guide*.

The WSS also requires an administrative certificate to enable WMS management access. If the switch does not already have certificates, WSS Software automatically generates them during the first system boot using WSS Software Version 4.2 or later. You do not need to install certificates unless you want to replace those automatically generated by WSS Software. (For more information, refer to "Certificates Automatically Generated by WSS Software" in "Managing Keys and Certificates" of the *Nortel WLAN 2300 System Software Configuration Guide*.)

Upload the WSS Configuration into a WMS Network Plan

Retrieve the basic configuration information added to the WSS and upload it into WMS.

To upload the WSS configuration into a WMS network plan

1. Select the Configuration tool bar option.
2. In the Task List panel, select Upload WSS.
3. In the IP Address box, type the IP address for the WSS.
4. In the Enable Password box, type the enable password for the WSS.

   This password must match the enable password that was defined using the CLI command **set enablepass**. For more information, see the *Nortel WLAN 2300 System Software Configuration Guide*.
5. Click **Next**. The uploading progress is shown.
6. After the Successfully uploaded device message is displayed, click **Next**.

   WMS uses its verification rules to check the switch's configuration. If an item in the configuration generates an error or warning, WMS displays the error or warning message.
7. Review the verification messages to determine whether you will need to make changes to the switch's configuration after uploading it into WMS.
8. Click **Next**.
9. Click **Finish**.

10 If WLAN Management Software displayed error or warning messages, select the Verification tool bar option. (Refer to "Verifying Configuration Changes" in the *Nortel WLAN Management Software 2300 Series Reference Guide*.)

Create a Service Profile

A service profile contains the configuration for the service you want to offer, such as employee access, guest access, or multi-hosted access.

For more information about service profiles, refer to "Wireless Configuration" on page 40. For more information about wireless services, refer to "Which Services to Provide?" on page 35.

To create a service profile

1 Select the Configuration tool bar option.

2 In the Organizer panel, click the plus sign next to the WSS.

3 Click the plus sign next to Wireless.

4 Select Wireless Services.

5 In the Task List panel, select one of the following:

- **802.1X Service Profile—Provides wireless access to 802.1X clients.**
- **Voice Service Profile—Provides wireless access to Voice over IP (VoIP) devices.**
- **Web-Portal Service Profile—Provides wireless access to clients who log in using a Web page.**
- **Open Access Service Profile—Provides wireless access to clients without requiring them to log in.**
- **Mesh Service Profile'**
- **Custom Service Profile—Provides wireless access based on the combination of option you choose. (Use this option only if none of the other options applies to the type of service you want to offer.)**

A wizard for configuring the service profile appears.

6 Read the first page of the wizard and click **Next**.

7 Edit the service profile and type an SSID name.

8 Edit additional settings as applicable to the type of service profile you are creating.

For information, refer to the following:

- **Chapter , "Configuring Wireless Services," on page 53**
- **"Viewing and Configuring Wireless Services" in "Configuring Wireless Parameters" of the** *Nortel WLAN Management Software 2300 Series Reference Guide*

9 Click **Finish**.

Create a Radio Profile and Map the Service Profile to It

To create a radio profile and map a service profile to that profile

1. Select the Configuration tool bar option.
2. In the Organizer panel, click the plus sign next to the WSS.
3. Click the plus sign next to Wireless.
4. Select Radio Profiles.
5. In the Task List panel under Create, select Create Radio Profile.
6. In the Name box, type the name of the radio profile (1 to 16 characters, with no spaces or tabs).
7. Click **Next**. Click **Next** again.
8. To map the radio profile to a service profile, select the service profile in the Available Service Profiles list and click **Add**.
9. Click **Finish**.

Create Your APs

Creating a *direct connect AP* or a *distributed AP* in your network plan in WMS depends on how the APs are connected to a WSS. A direct connect AP is connected to the wired network through a direct 10/100 Ethernet connection to a WSS. A distributed AP is connected to the WSS indirectly through other Layer 2 or Layer 3 wired networking devices.

To create a directly connected AP in WMS

1. Access the Create Direct-Connect AP wizard
   a. Select the Configuration tool bar option.
   b. In the Organizer panel, click the plus sign next to the WSS.
   c. Click the plus sign next to Wireless.
   d. Select Access Points.
   e. In the Task List panel, select Directly Connected AP.
2. Select the WSS port the AP will be connected to from the Available Ports drop-down list.

Note. Configuring a directly connected AP in a port converts the port to an AP access port. If the port is a statically configured member of a VLAN, the port is removed from the VLAN.

3 Click **Next**.

4 Select the AP model from the AP Model list.

5 To select the radio type for a single-radio model, click the AP Radio Type box and select one of the following radio types:

- **11b—802.11b only**
- **11g—802.11b/g**

6 Click **Next**.

Note. The non-editable number (1 or 2) indicates the radio number on the AP.

7 To select the radio type for a single-radio model, click the AP Radio Type box and select one of the following radio types:

- **11b—802.11b only**
- **11g—802.11b/g**

8 Click **Next**.

9 Configure the radios

a To enable the radio, select **Enabled**.

b In the Radio Profile list, select the profile to which the radio belongs.

c In the Channel Number list, select the channel number for the radio.

Note. If RF Auto-Tuning for channel configuration is enabled, setting this value has no effect. The channel number is controlled by RF Auto-Tuning.

d In the Transmit Power box, specify the transmit power for the radio.

Note. If RF Auto-Tuning for power configuration is enabled, setting this value has no effect. The power level is controlled by RF Auto-Tuning.

e If the AP has two radios, click **Next** and go to step 10. Otherwise, go to step 11.

10 Click **Finish**.

To create a Distributed AP in WMS

1 Access the Create AP wizard

a Select the Configuration tool bar option.

b In the Organizer panel, click the plus sign next to the WSS.

c Click the plus sign next to Wireless.

d Select Access Points.

e In the Task List panel, select AP.

2 In the Name box, type a name (1 to 16 alphanumeric characters, with no spaces or tabs).

3 In the DAP Number box, specify the connection number for the WSS's connection to this Distributed AP. The range of valid connection numbers depends on the WSS model as follows:

- **For a 2382, you can specify a number from 1 to 320.**
- **For a 2380, you can specify a number from 1 to 300.**
- **For a 2360/2361, you can specify a number from 1 to 30.**
- **For a 2350, you can specify a number from 1 to 8.**

4 In the Serial Number box, type the serial number of the AP.

5 In the Fingerprint box, type the 16-digit hexadecimal number of the AP's encryption fingerprint. Use one of the following formats:

- **11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:00**
- **1122:3344:5566:7788:99aa:bbcc:ddee:ff00**

An AP's fingerprint is the hash value of the AP's public encryption key. The fingerprint is displayed on a label on the back of the AP, and is labeled *RSA key*. If the AP is already installed and operating, use the CLI command **show dap status** command to display the fingerprint.

Note. The fingerprint is used for secure communication between the WSS and the AP and applies only to Distributed APs.

6 Click **Next**.

7 Select the AP model from the AP Model list.

8 To select the radio type for a single-radio model, click the AP Radio Type box and select one of the following radio types:

- **11b—802.11b only**
- **11g—802.11b/g**

9 Click **Next**.

10 Configure the radios

a To enable the radio, select **Enabled**.

b In the Channel Number list, select the channel number for the radio.

Note. If RF Auto-Tuning for channel configuration is enabled, setting this value has no effect. The channel number is controlled by RF Auto-Tuning.

c In the Transmit Power box, specify the transmit power for the radio.

Note. If Auto-RF for power configuration is enabled, setting this value has no effect. The power level is controlled by Auto-RF.

d If the AP has two radios, click **Next** and go to step 10. Otherwise, go to step 11.

11 Click **Finish**.

Apply a Radio Profile to Each Radio

When you create an AP, a new radio (or radios, depending upon the type of AP created) is added into WMS. The radios use the default radio profile in WMS unless you create a new radio profile and apply it to each radio on the AP.

For more information about creating a radio profile, refer to "Create a Radio Profile and Map the Service Profile to It" on page 104. For more information about creating an AP, refer to "Create Your APs" on page 104.

To apply a radio profile to a radio

1 Select the Configuration tool bar option.
2 In the Organizer panel, click the plus sign next to the WSS.
3 Click the plus sign next to Wireless.
4 Select Radio Profiles.
5 In the Radio Profiles table, select the radio profile.
6 Click **Properties**.
7 Click the Radio Selection tab.
8 Select the radios in the Available Members list and click **Move**.
9 Click **OK**.

You have completed the necessary steps for configuring your RF environment.

What's Next?

After creating the services (Refer to "Configuring Wireless Services" on page 53.) and following the instructions in this chapter to create the RF environment, deploy the configuration and enable monitoring. Optionally, you can improve your network monitoring options by modelling your floor and defining RF obstacles.

- For information about monitoring your network, refer to "Managing and Monitoring Your Network" on page 161.
- For information about enhancing Auto-RF with modelling to better define your site and improve monitoring options, refer to "Using Auto-RF with Modelling" on page 109.

Using Auto-RF with Modelling

What Is Auto-RF with Modelling? 109
Add Site Information 109
Insert RF Obstacles 113
Create Your RF Coverage Area 115
What's Next? 127

What Is Auto-RF with Modelling?

Auto-RF with modelling is a technique you can use to configure and implement your network. This technique builds on the Auto-RF method. You will still use Auto-RF (auto tuning) to adjust power and channel settings, which provides RF signals to the coverage area. After using Auto-RF, provide modelling information about your geographic location to enhance the auto tuning feature.

To use this technique, complete the tasks described in "Using Auto-RF" on page 101then complete the following steps:

1. Add site information (buildings and floors) or import a floor drawing.
2. Add RF obstacles (optional).
3. Add an RF coverage area.

By providing some information about your buildings and floors, WMS gains the information to better visualize the network topology and support improved monitoring.

To learn more about the benefits of Auto-RF with modelling, refer to "Auto-RF with Modelling" on page 37.

Add Site Information

Note. The RF Planning software does not support outdoor installations. Results obtained do not compensate nor account for obstacles and characteristics typically associated with outdoor environments. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.

By adding minimal information about your buildings and floors at your site, you support improved monitoring for your network. Manually add building and floor information or import a floor plan. For information about importing a floor plan, refer to "Import a Floor Plan" on page 136.

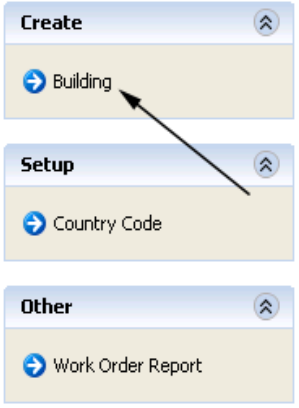
To add site information

1. Select the RF Planning tool bar option.
2. In the Organizer panel, click the name of the network plan.
3. Select Site in the Task List panel. The Create Site wizard, a series of dialog boxes, prompts you for information about the new site.
4. In the Site Name box, type a name for the site (1 to 80 alphanumeric characters, with no spaces or tabs), and click **Next**.
5. To change the Country Code, select the country where the network is to be deployed in the Country Code list.
6. In the Channel Set (802.11b/g) list, select the set of operating channels for any 802.11b/g AP radios you plan to use (if different from the default), and click **Next**.
7. In the Number Of Buildings box, specify how many buildings are in your site, and click **Finish**.

   When you specify the number of buildings a site contains, WLAN Management Software creates each building using the default settings. You can edit the buildings WLAN Management Software creates or you can add new buildings.

To create a building

1. In the Organizer panel, click the site name.
2. Select Create Building in the Task List panel. The Create Building wizard prompts you for information about the new building.



3. In the Building Name box, type the name of the building (1 to 30 alphanumeric characters, with no spaces or tabs), and click **Next**.
4. In the Number Of Floors box, specify how many floors the building has.

   When you specify the number of floors a building contains, WLAN Management Software creates each floor using the default settings. You can edit the floors WLAN Management Software creates or you can add new floors.

5 In the Starting Floor Level box, specify the floor number of the first floor in the building. To start with a subterranean floor, you can specify 0 or a negative floor number.

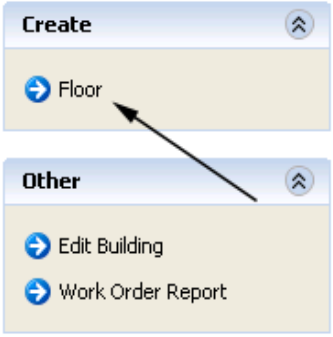
6 In the Skip Floor Levels box, specify floor numbers you want to skip. Skipping floors is useful when you want to model only certain floors in a building. Use commas to separate the floor numbers in a list; for example: 1,3,7 Use a hyphen when entering a range; for example: 8-12.

7 Click **Finish** to close the wizard.

To add a floor to the building

1 In the Organizer panel, click the building name.

2 Select Floor in the Task List panel. The Create Floor wizard prompts you for information about the new floor.



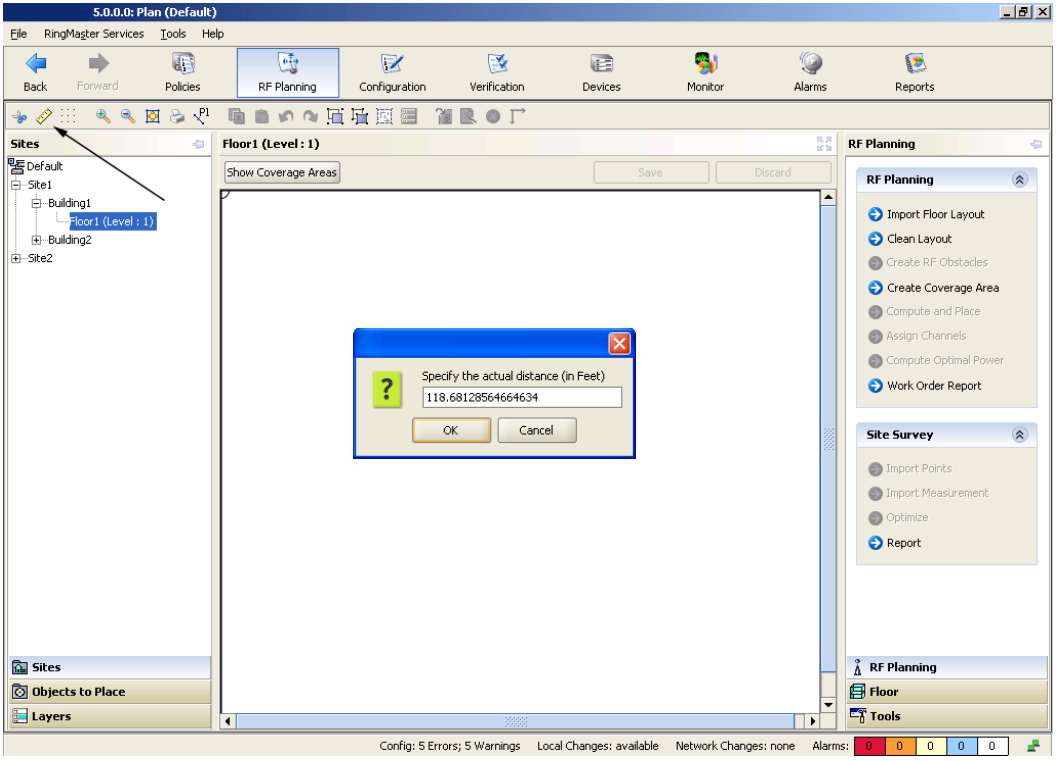
3 In the Floor Name box, type the name of the floor (1 to 60 alphanumeric characters, with no spaces or tabs), and click **Next**.

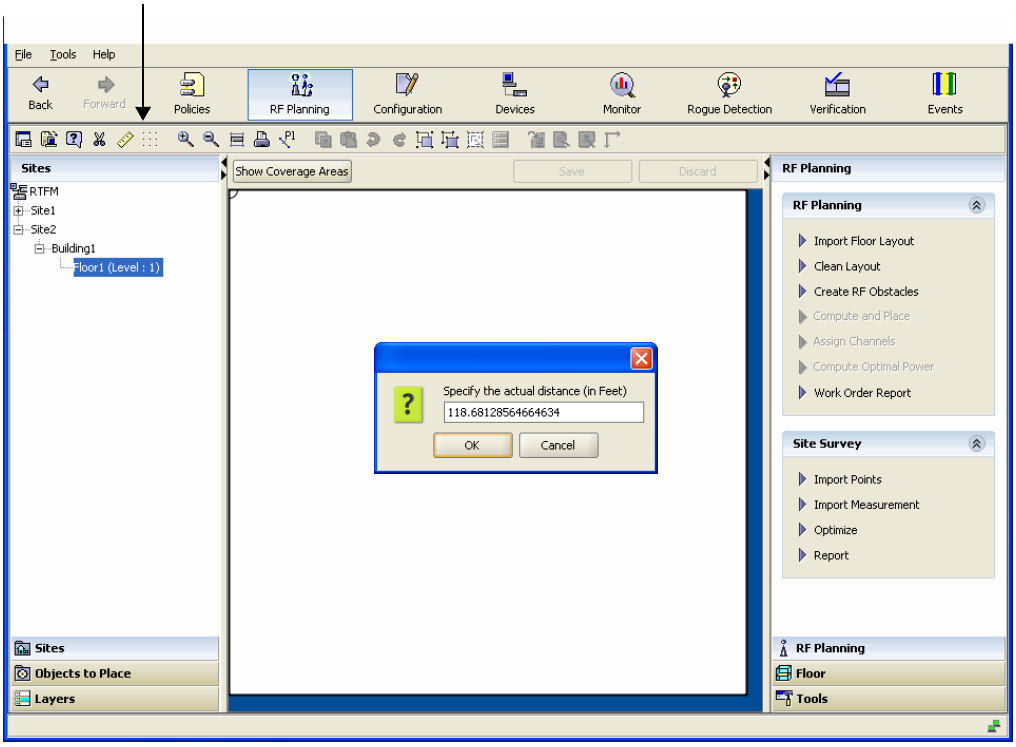
4 To change the default attenuation for radios, type the number of dB in the 802.11a (dB) box or 802.11b/g (dB) box.

5 In the Height of the Ceiling box, type the number of feet or meters from the floor to the ceiling (1 to 1000 feet or meters).

6 Click **Finish** to close the wizard.

7 When you click on the floor's name in the Organizer panel, a view of the floor plan is displayed in the Content panel. Click on the ruler icon to set the scale of your floor.





Insert RF Obstacles

Note. The RF Planning software does not support outdoor installations. RF obstacles typically found in outdoor environments have not been adequately tested for their attenuation characteristics. As a result, the database cannot ensure accurate attenuation coefficients for RF planning purposes. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.

Add major RF obstacles that will affect the placement of your APs, such as solid walls, barriers, or elevator shafts.

To add RF obstacles

1. Display the floor plan in the Content panel.
2. In the Task List panel, click Tools.

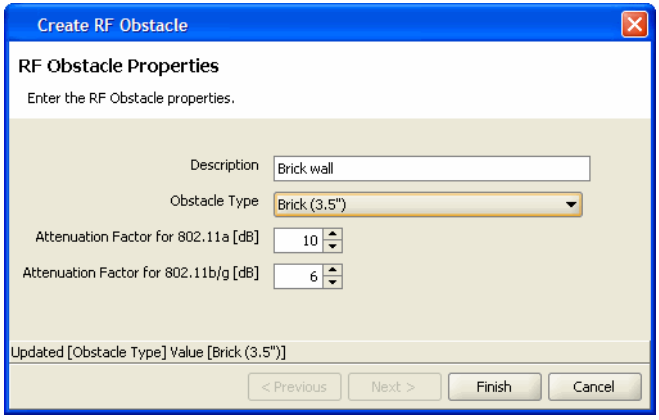
3 In the RF Obstacle area under Layout, click one of the icons that most closely matches the RF obstacle you wish to place.

4 Click and drag the mouse to draw the location and shape of the RF obstacle on the floor.

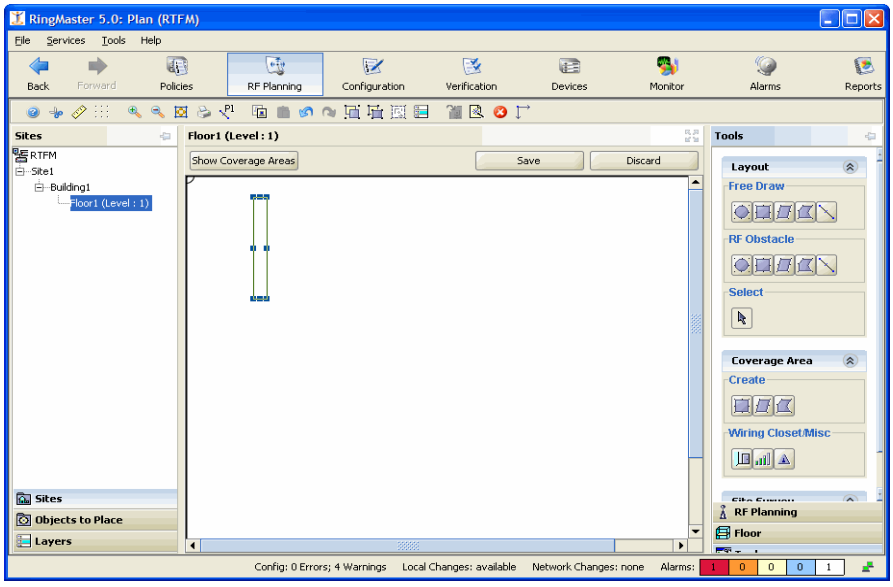
The Create RF Obstacle wizard is displayed.

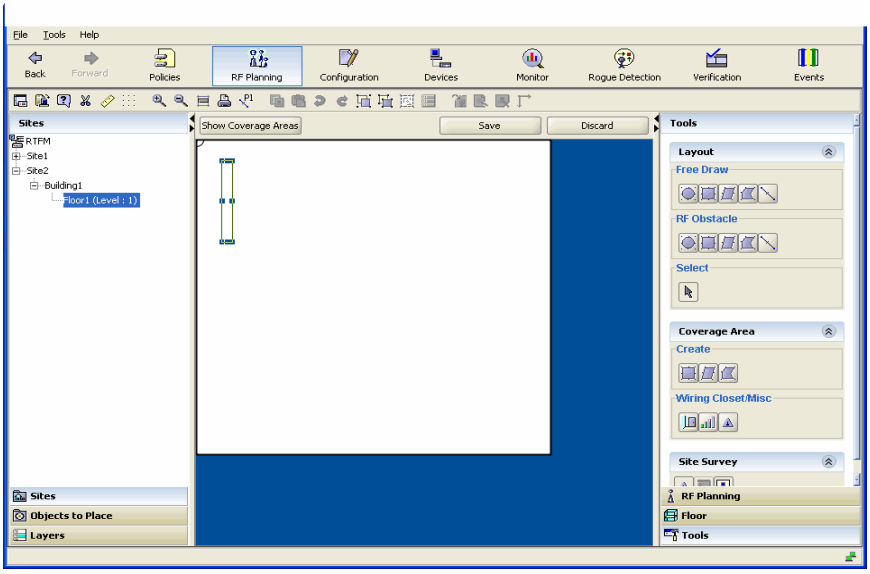
5 Enter a description of the RF obstacle, and select the Obstacle Type from the list.

A default attenuation factor is displayed for the object type, or, you can select an attenuation factor that you believe more closely matches the RF obstacle.



6 Click **Finish**. The RF obstacle is added to your floor layout.





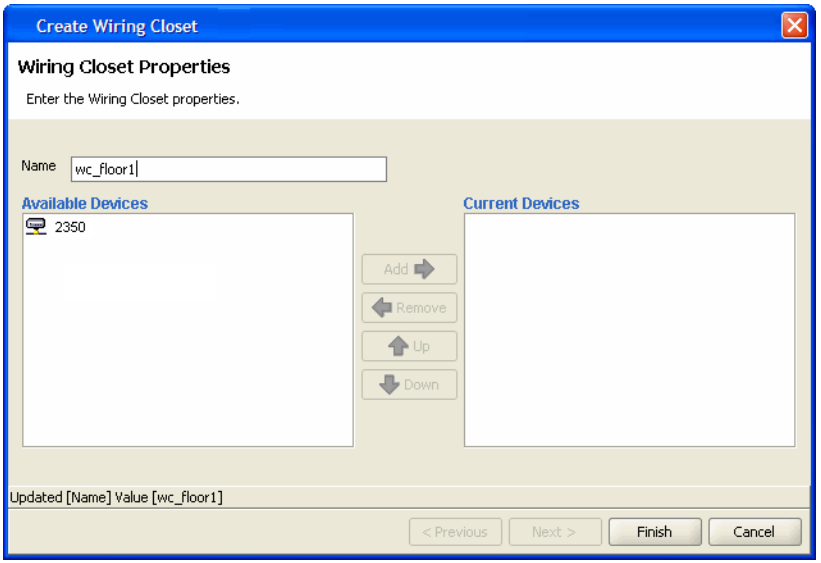
Create Your RF Coverage Area

To create your RF coverage area, create a wiring closet (mandatory if you have direct APs), designate an area for RF coverage, and add *distributed APs* or *direct APs* to the coverage area. Distributed APs are indirectly attached through intermediate Layer 2 or Layer 3 devices. Direct APs are directly attached to dedicated WSS ports.

Create a Wiring Closet

To add the location of a wiring closet to the floor plan

1. Display the floor plan in the Content panel.
2. In the Task List panel, click Tools.
3. In the Wiring Closer/Misc area under Coverage Area, click the (Insert Wiring Closet) icon.
4. Click in the floor display where you want to place the wiring closet. The Create Wiring Closet wizard appears.



5 In the Name box, type the name of the wiring closet (1 to 60 characters, with no tabs).

6 Click a WSS in the Available Devices box, then click the **Add** button to move it to the Current Devices box.

7 Click **Finish** to save the changes. The wiring closet is displayed on your floor plan.

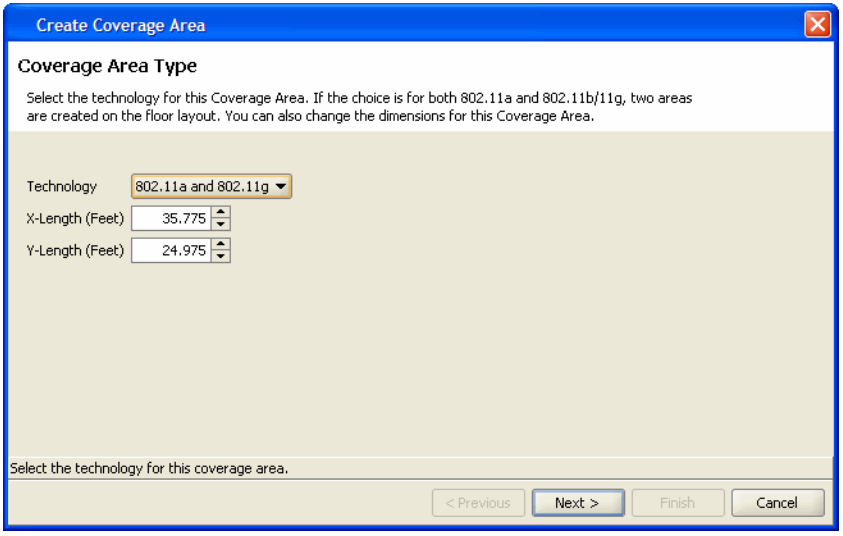
Create Your RF Coverage Area

To create your RF coverage area

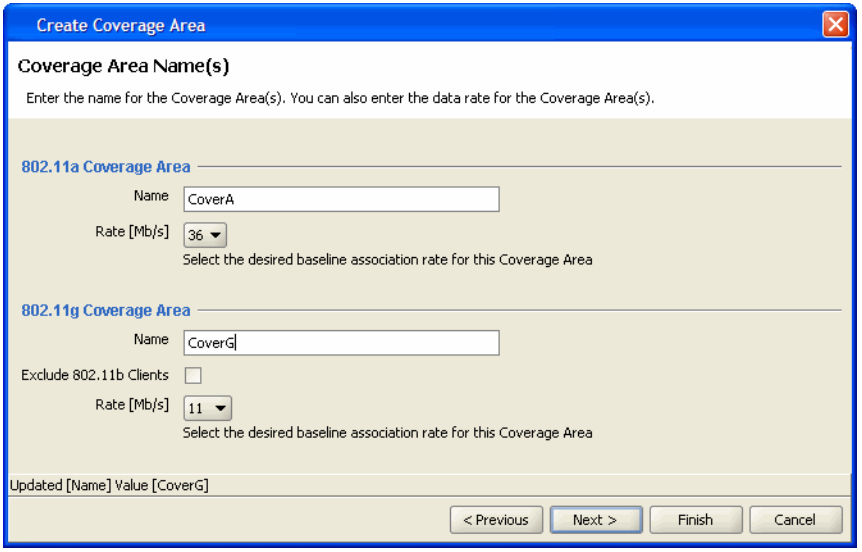
1 Display the floor plan in the Content panel.

2 In the Task List panel, click Tools.

3 In the Create field under Coverage Area, click one of the icons and draw the RF coverage area you want to add to the floor by clicking and dragging the mouse. The Create Coverage Area wizard appears.


Create Coverage Area
Coverage Area Type
Select the technology for this Coverage Area. If the choice is for both 802.11a and 802.11b/11g, two areas are created on the floor layout. You can also change the dimensions for this Coverage Area.
Technology
802.11a and 802.11g
X-Length (Feet)
35.775
Y-Length (Feet)
24.975
Select the technology for this coverage area.
< Previous
Next >
Finish
Cancel

4 Select one or more technologies to use in the coverage area. Click **Next**. The wizard presents properties and association pages for the technology in step 3.



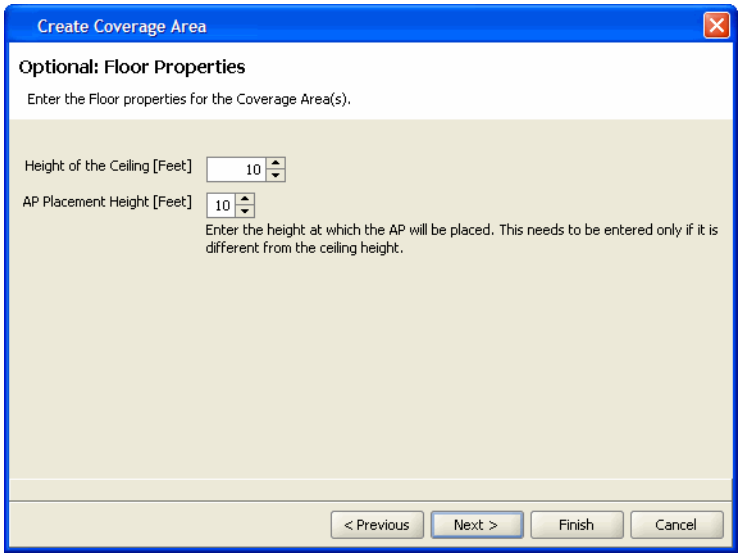
5 In the Name box for each technology, type a name for the coverage area (1 to 60 characters long, with no tabs).

6 In the Rate [Mb/s] list for each technology, select the average desired association rate for typical clients in this coverage area.

7 For 802.11g, to prevent the association of 802.11b clients to any radio in this coverage area, select **Exclude 802.11b clients**. To allow 802.11b clients to associate to radios in the coverage area, clear **Exclude 802.11b clients**.

Note. Even when association of 802.11b clients is disabled, if an 802.11b/g radio detects a beacon from an 802.11b network, the radio enters protection mode to protect against interference.

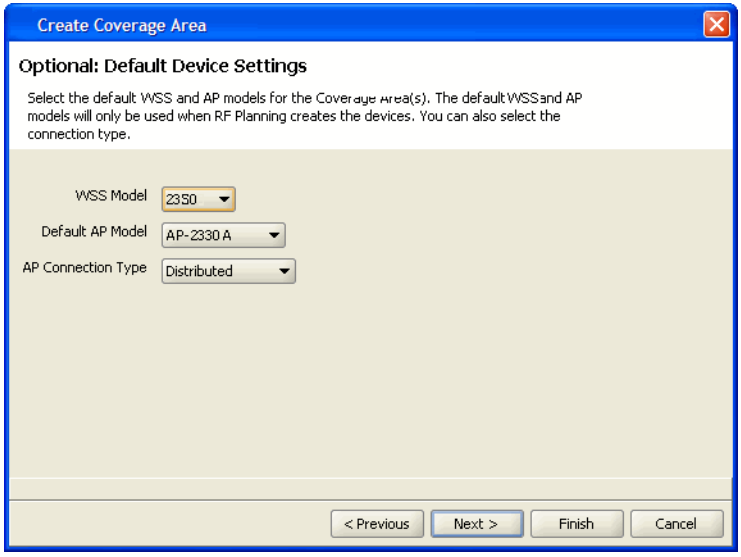
8 Click **Next**. The Floor Properties page appears.


Create Coverage Area
Optional: Floor Properties
Enter the Floor properties for the Coverage Area(s).
Height of the Ceiling [Feet]
10
AP Placement Height [Feet]
10
Enter the height at which the AP will be placed. This needs to be entered only if it is different from the ceiling height.
< Previous
Next >
Finish
Cancel

9 To change the ceiling height, specify the new height in the Height of the Ceiling box.

10 To change the height where APs are mounted, specify the new mounting height in the AP Placement Height box.

11 Click **Next**. The Default Device Settings page appears.


Create Coverage Area
Optional: Default Device Settings
Select the default WSS and AP models for the Coverage Area(s). The default WSS and AP models will only be used when RF Planning creates the devices. You can also select the connection type.
WSS Model
2350
Default AP Model
AP-2330 A
AP Connection Type
Distributed
< Previous
Next >
Finish
Cancel

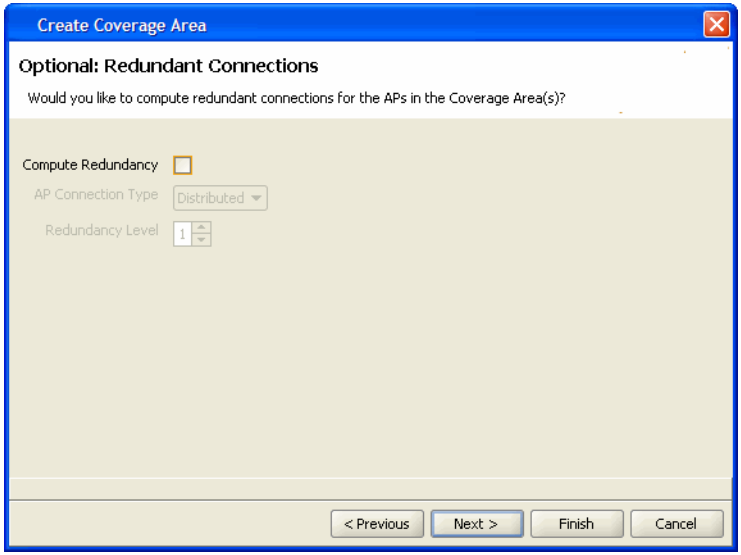
12 To change the default WSS model, select the model from the WSS Model list.

13 To change the default AP model, select the model from the Default AP Model list.

14 To change the AP connection type, select the one of the following types from the AP Connection Type list:

- **Direct—APs are directly attached to dedicated WSS ports.**
- **Distributed—APs can be indirectly attached through intermediate Layer 2 or Layer 3 devices.**
- **Distributed (Auto)—APs can be indirectly attached through intermediate Layer 2 or Layer 3 devices. WMS automatically configures the APs using a profile that assigns a Distributed AP number and name to the AP from among the unused valid AP numbers available on the switch.**

15 Click **Next**. If you selected Direct or Distributed in the AP Connection Type list, the Redundant Connections page appears. Go to step 16. If you selected Distributed (Auto) in the AP Connection Type list, the Capacity Planning for Data page appears. Go to step 20.



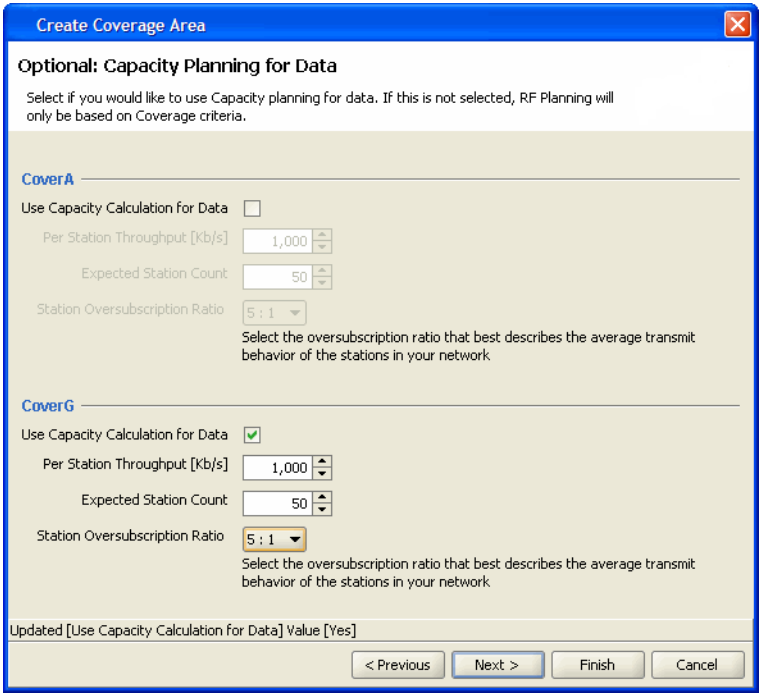
16 To plan for redundant AP connections to WSSs, select **Compute Redundancy**.

17 To change the AP connection type for the redundant connection, select **Direct** or **Distributed** from the AP Connection Type list.

18 To change the number of redundant connections for the distributed connection type, type the number in the Redundancy Level box.

For direct connections, the redundancy level is always 1.

19 Click **Next**. The Capacity Planning for Data page appears.


Create Coverage Area
Optional: Capacity Planning for Data
Select if you would like to use Capacity planning for data. If this is not selected, RF Planning will only be based on Coverage criteria.
CoverA
Use Capacity Calculation for Data
Per Station Throughput [Kb/s]
1,000
Expected Station Count
50
Station Oversubscription Ratio
5 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the stations in your network
CoverG
Use Capacity Calculation for Data
Per Station Throughput [Kb/s]
1,000
Expected Station Count
50
Station Oversubscription Ratio
5 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the stations in your network
Updated [Use Capacity Calculation for Data] Value [Yes]
< Previous
Next >
Finish
Cancel

20 To calculate AP placement and configuration based on both coverage and on capacity, enable **Use Capacity Calculation for Data**. Otherwise, click **Next** and go to step 24.

By default, WLAN Management Software performs only the coverage calculation. If you enable the **Use Capacity Calculation for Data** option, WLAN Management Software performs both calculations.

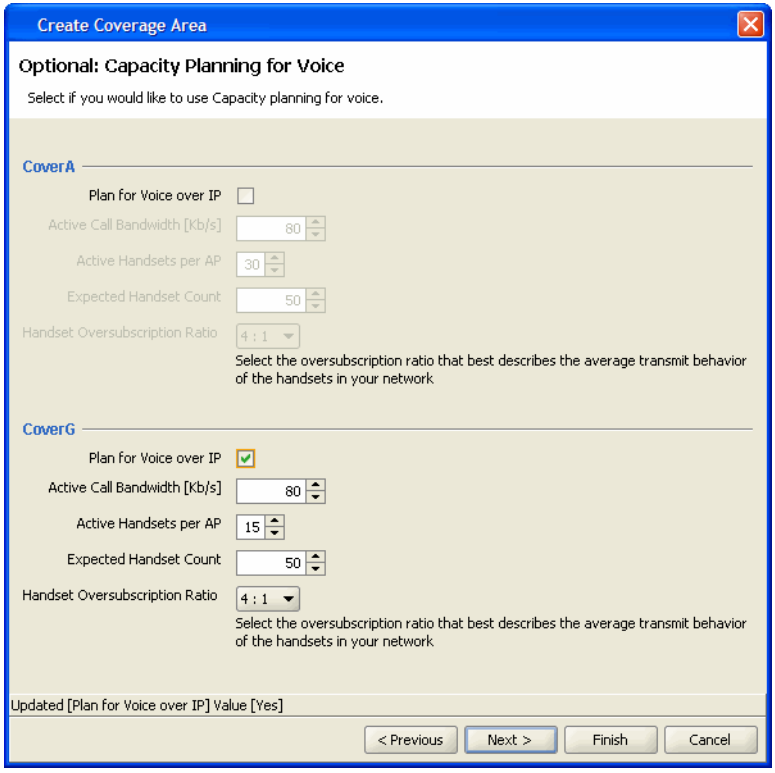
21 In the Per Station Throughput list, specify the throughput (combined transmit and receive) in kilobits per second (Kbps) for a station.

22 In the Expected Station Count list, specify the number of clients expected to be in the coverage area.

23 In the Station Oversubscription Ratio list, select the ratio for the average transmit behavior of the stations.

The station oversubscription ratio is the ratio of active clients compared to total clients. For example, the ratio 5:1 indicates that, statistically, 20 percent of the clients are active at any given time.

24 Click **Next**. The Capacity Planning for Voice page appears.


Create Coverage Area
Optional: Capacity Planning for Voice
Select if you would like to use Capacity planning for voice.
CoverA
Plan for Voice over IP
Active Call Bandwidth [Kb/s]
80
Active Handsets per AP
30
Expected Handset Count
50
Handset Oversubscription Ratio
4 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the handsets in your network
CoverG
Plan for Voice over IP
Active Call Bandwidth [Kb/s]
80
Active Handsets per AP
15
Expected Handset Count
50
Handset Oversubscription Ratio
4 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the handsets in your network
Updated [Plan for Voice over IP] Value [Yes]
< Previous
Next >
Finish
Cancel

25 To calculate AP placement and configuration based on both coverage and capacity for voice over IP, enable **Plan for Voice over IP**. Otherwise, click **Next** and go to step 30

By default, WLAN Management Software performs only the coverage calculation. If you enable the **Plan for Voice over IP** option, WLAN Management Software performs both calculations.

26 In the Active Call Bandwidth list, specify the amount of bandwidth in kilobits per second (Kbps) that you expect for each call.

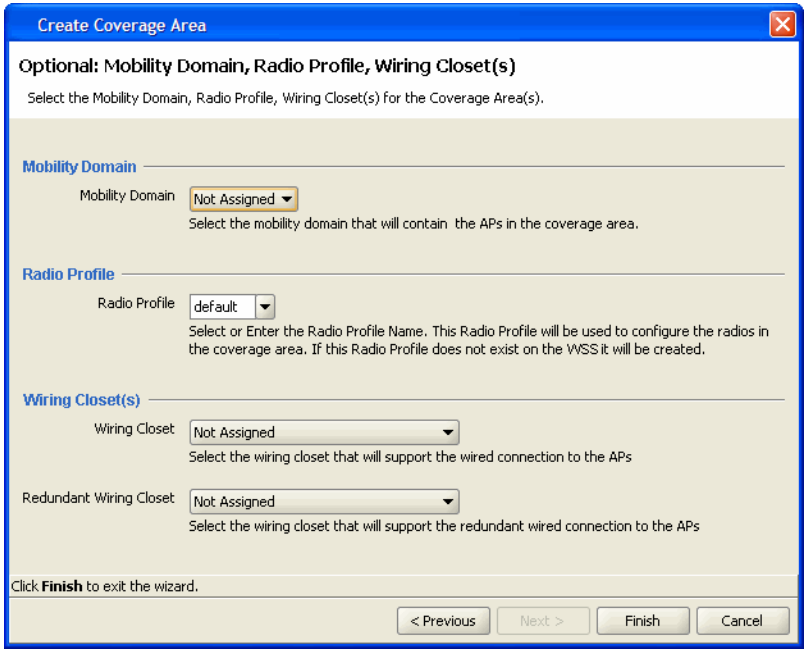
27 In the Active Handsets per AP list, specify the number of voice over IP phones that you want each AP to handle.

28 In the Expected Handset Count list, specify the number of voice over IP phones you expect to be in the coverage area.

29 In the Handset Oversubscription Ratio list, select the ratio for the average transmit behavior of the voice over IP phones.

The handset oversubscription ratio is the ratio of active handsets compared to total handsets. For example, the ratio 4:1 indicates that, statistically, 25 percent of the voice over IP phones are active at any given time.

30 Click **Next**. The Mobility Domain, Radio Profile, Wiring Closet(s) page appears.


Create Coverage Area
Optional: Mobility Domain, Radio Profile, Wiring Closet(s)
Select the Mobility Domain, Radio Profile, Wiring Closet(s) for the Coverage Area(s).
Mobility Domain
Mobility Domain
Not Assigned
Select the mobility domain that will contain the APs in the coverage area.
Radio Profile
Radio Profile
default
Select or Enter the Radio Profile Name. This Radio Profile will be used to configure the radios in the coverage area. If this Radio Profile does not exist on the WSS it will be created.
Wiring Closet(s)
Wiring Closet
Not Assigned
Select the wiring closet that will support the wired connection to the APs
Redundant Wiring Closet
Not Assigned
Select the wiring closet that will support the redundant wired connection to the APs
Click Finish to exit the wizard.
< Previous
Next >
Finish
Cancel

31 In the Mobility Domain list, select the Mobility Domain that contains the APs used for this coverage area.

32 In the Radio Profile list, select the radio profile used for this coverage area.

The profiles available depend on the Mobility Domain you selected in step 31. The profile you select applies to all radios associated with the coverage area. If you type the name of a radio profile that does not already exist, WLAN Management Software creates it.

33 In the Wiring Closet list, select the wiring closet that contains the WSS or switches to be connected to the shared AP.

If the APs will be directly connected to WSSs, a wiring closet is required. If all the APs in the coverage area will be indirectly connected to WSSs through the network, a wiring closet is not required.

34 In the Redundant Wiring Closet list, select the wiring closet that will provide redundant connection to the AP. This is required for directly connected APs, if you require the APs to have redundant connections. Otherwise, this is not required.

35 Click **Finish** to complete the wizard and create the coverage area. The coverage area is now displayed on your floor.

Add APs

Add your direct APs or distributed APs to your network.

To add direct APs or distributed APs to your network

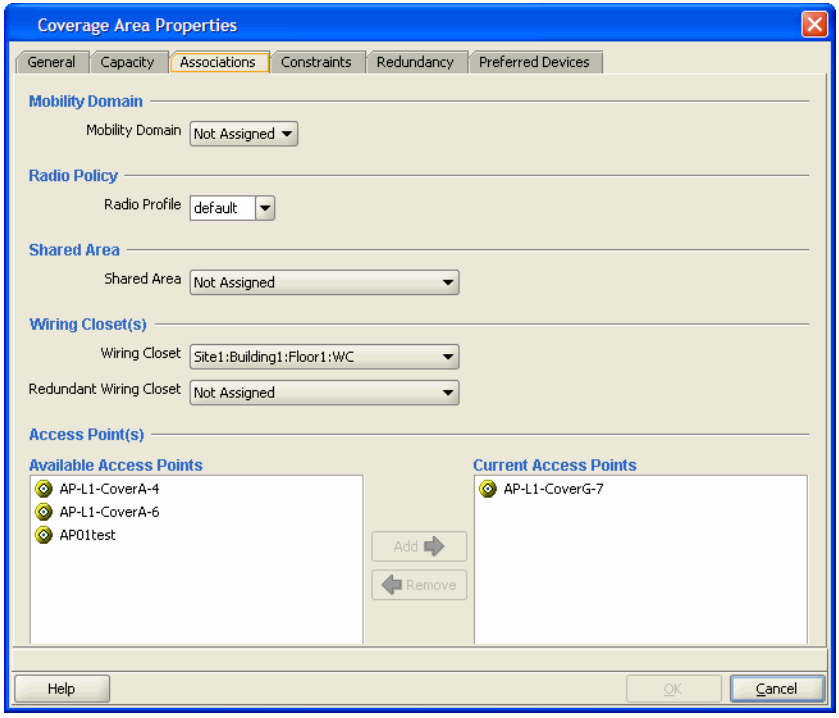
1. If you have not already done so, create a wiring closet and associate your WSSs to the closet. For more information, refer to "Create a Wiring Closet" on page 115.
2. Go to "Create Your APs" on page 104 for information about adding direct APs or distributed APs to your network. Once created, APs can be associated with a coverage area and added to the floor plan.

Associate APs to the Coverage Area

Associate both your distributed APs and direct APs to a coverage area on the floor.

To associate APs to the coverage area

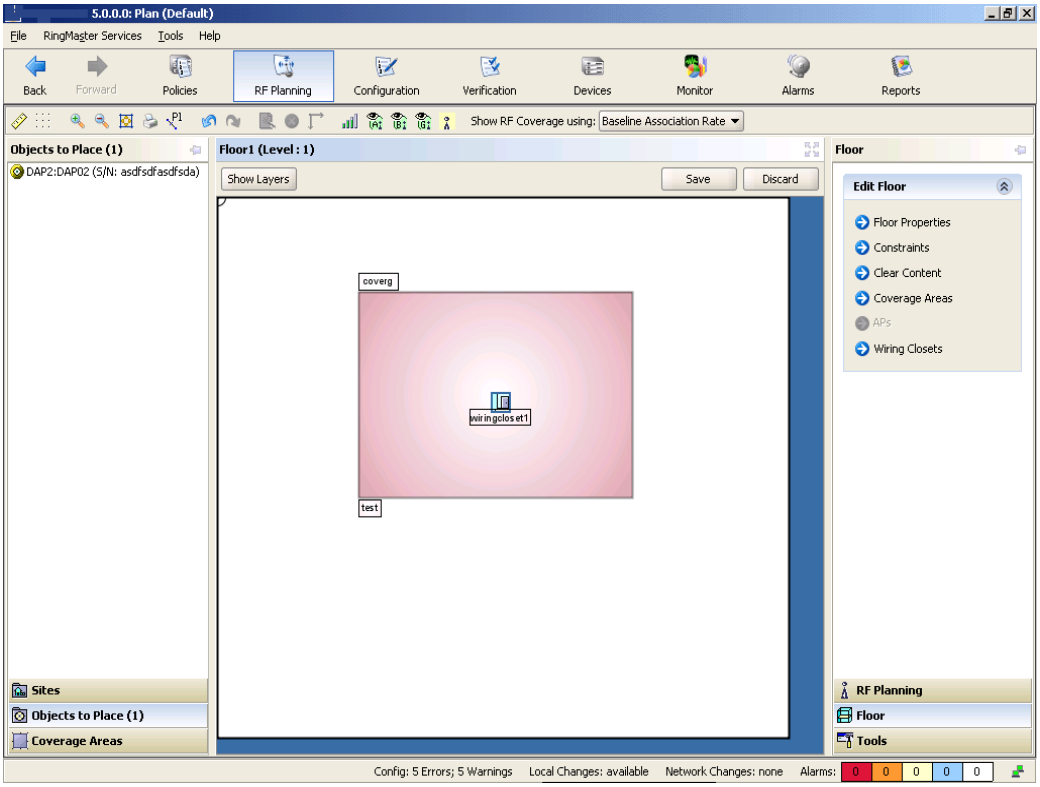
1. Select the RF Planning tool bar option.
2. In the Content panel, display the floor plan where the APs are to be installed.
3. In the Organizer panel, click on Coverage Areas.
4. Right-click the Coverage Area to which the APs are to be associated, and select Edit Properties from the menu. The Coverage Area Properties dialog for the selected coverage area appears.
5. Click the Associations tab to display area associations information for the coverage area.

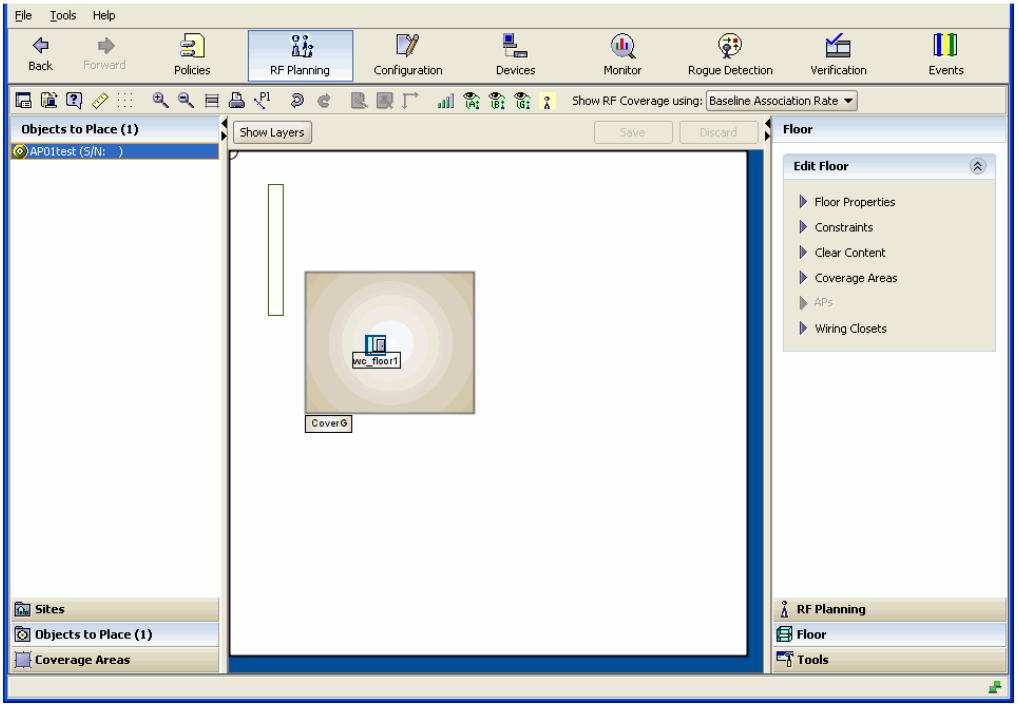


6 In the Available Access Points box, select one or more available APs to use in the coverage area, then click **Add** to move the APs to the Current Access Points box.

7 Click **OK** to close the dialog box.

8 In the Organizer panel, click on Objects to Place. A list of the APs you created is displayed in the panel.





9 Click on the AP icon, then click on the location where you installed the AP. The AP icon moves from the Objects To Place panel to its location on the floor.

What's Next?

This section provides cross references to information on the following tasks:

- "Using RF Planning" on page 129
- "Managing and Monitoring Your Network" on page 161

Using RF Planning

What Is RF Planning? 129
Prepare the Floor Drawings 130
Define Site Information 131
Model RF Obstacles 140
Import a Site Survey 142
Plan RF Coverage 142
Generate a Work Order 157
Install the Equipment 158
What's Next? 159

What Is RF Planning?

RF Planning is a technique used to import detailed information about your site into WMS. In addition, you can use RF Planning to add RF obstacle information and third-party APs and configure your RF coverage area at a finer level than is possible using the Auto-RF with modelling technique.

By defining sites, buildings, and floors, you provide WMS with the necessary information to modularly manage large networks based on geographical or organizational boundaries. For example, a network plan can represent a campus-wide network. Nortel recommends that you limit a network plan to a single campus or Mobility Domain. A network plan is also limited to one country, since a network plan only supports one common country code for the WSSs contained in it.

Note. The RF Planning software does not support outdoor installations. RF obstacles typically found in outdoor environments have not been adequately tested for their attenuation characteristics. As a result, the database cannot ensure accurate attenuation coefficients for RF planning purposes. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.

Perform the following steps to use the RF planning technique:

1. Prepare your floor plan graphic files
2. Add site information
3. Add RF obstacles
4. Add an RF coverage area
5. Create a work order
6. Install your equipment
7. Deploy your configuration

To learn more about the benefits of RF Planning, refer to "RF Planning" on page 37.

Prepare the Floor Drawings

Note. If your floor drawings are contained in JPEG or GIF files, this step does not apply. Go directly to "Define Site Information" on page 131.

If you plan to import AutoCAD DXF™ or AutoCAD DWG files into WMS, you should perform some "clean up" work before importing the files. Doing this work before you import the files into WMS creates a more compact file, requiring less storage space. Typically, the more CAD diagram cleanup that is done within the CAD software, the more smoothly the drawing will import into WMS.

Perform the following steps to clean up the AutoCAD file:

1. Perform an audit
2. Turn on, unlock, and unfreeze all layers
3. Remove unnecessary notations
4. Purge unused blocks, line types, and layers

Typically, based on the drawing technique chosen when the drawing file was created in AutoCAD or TurboCAD, a single object might be drawn with more than one line; for example, walls. When such an object is imported, it results in more than one object in WMS. To avoid the actual object being defined as more than one obstacle, delete parallel lines within a certain distance.

Another method you can use to achieve the same result is to group all the lines into one object. For example, you might group four lines that form an office or conference room to create one attenuation factor for that entire area. Or, group multiple lines that were drawn in the floor plan to create a bigger line.

Grouping lines is not always recommended. For example, grouping lines into one object does not work well with polylines. Grouped polylines are recognized by the planning tool in WMS as a single, monolithic obstacle. This causes incorrect results when viewing RF coverage.

Note. Objects must not be RF Obstacles or Groups before Clean Layout is performed.

After you import the file into WMS, you have the opportunity to remove any unnecessary objects overlooked during your initial preparation of the floor drawings. To do this, you can use the Clean Layout feature and other editing tools in the Building wizard.

For more information about how to prepare the AutoCAD files for WMS. refer to the *Nortel WMS Reference Manual*.

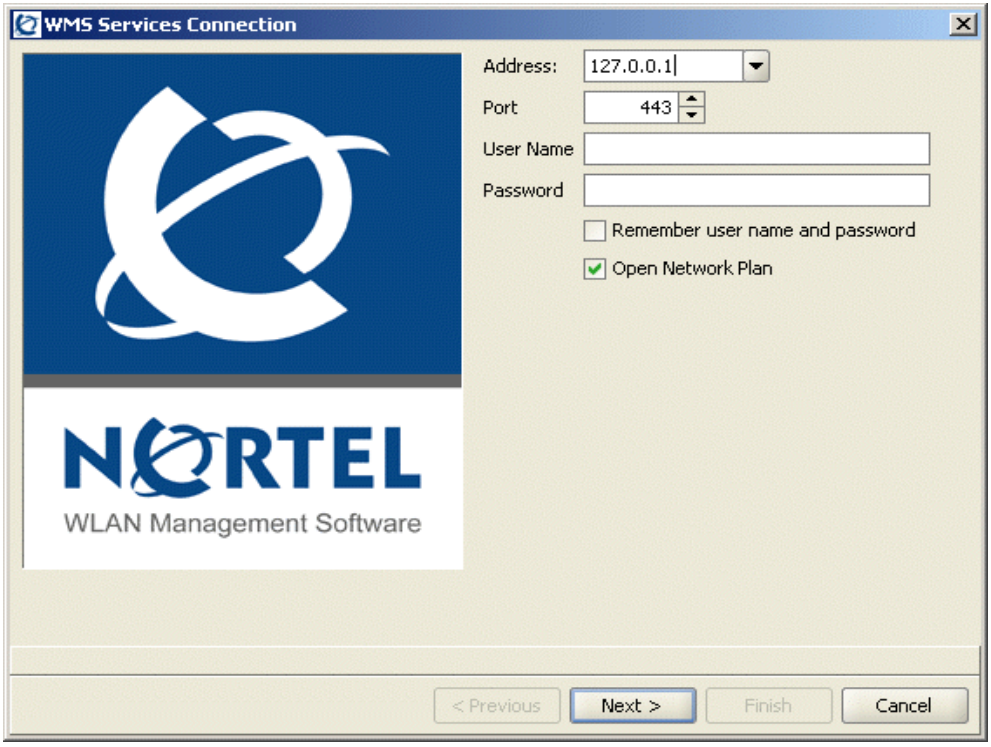
Define Site Information

You define your site with information about your campus, buildings, and floors. In addition, you describe the attenuation characteristics of the location and specify the traffic engineering needs (bandwidth and reliability) of the users.

Note. WLAN Management Software commits your work into the network plan only when you click **Finish**, not when you click **Next**. Changes are not persistently saved until you save the network plan.

To create a network plan

1. Connect to a host running WLAN Management Software Services. When you start WLAN Management Software, the WLAN Management Software main window and the WLAN Management Software Services Connection dialog box appear.

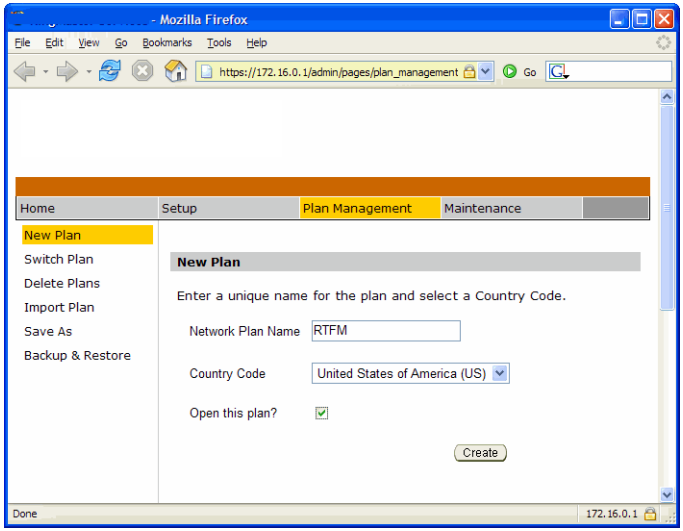


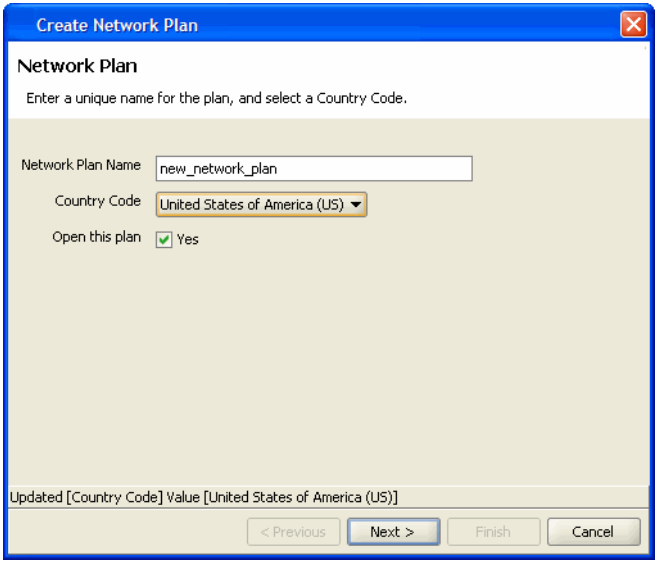
2. In the WMS Services Connection dialog box, enter the IP address of a host running WMS Services, optionally enter a user name and password, and click **Next**.

   If the WMS Service is installed on the same machine as the one you are using to run WLAN Management Software, enter 127.0.0.1 as the IP address. This is a standard IP loopback address.

3. After a connection is established to the specified WMS Services host, select **Services > Plan Management**. The WMS Services Plan Management page is displayed in a browser window.

4. In the left-hand column of the page, click New Plan. The New Plan page is displayed.





5 In the Network Plan Name box, type a name for the network plan. You can use 1 to 60 alphanumeric characters with no spaces, tabs, or any of the following: slash (/), backslash (\), quotation marks (“ ”), asterisk (*), question mark (?), angle brackets (< >), or vertical bar (|).

6 In the Country Code list, select the country where the network is to be deployed.

Note. You *must* select a country code before continuing.

7 Select the **Open this plan?** checkbox to open the plan in WLAN Management Software.

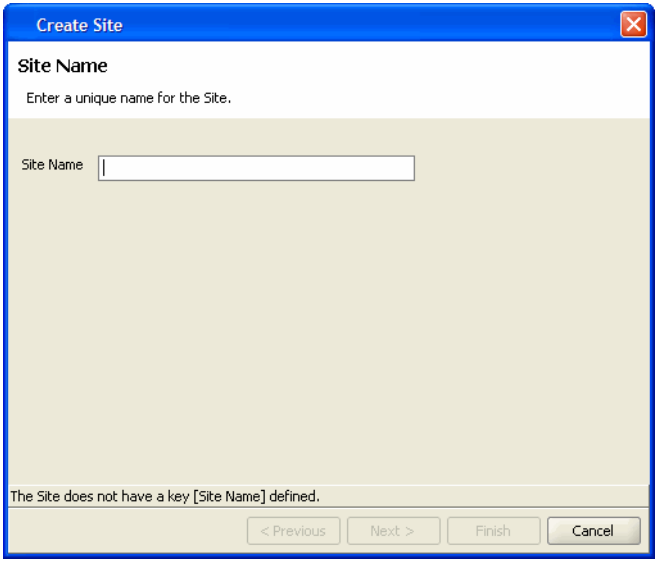
8 Click Create to create the new network plan.

To add site information

1 Select the RF Planning tool bar option.

2 In the Organizer panel, click the name of the network plan.

3 Select Create Site in the Task List panel. The Create Site wizard, a series of dialog boxes, prompts you for information about the new site.



4 In the Site Name box, type a name for the site (1 to 80 alphanumeric characters, with no spaces or tabs), and click **Next**.

5 To change the Country Code, select the country where the network is to be deployed in the Country Code list.

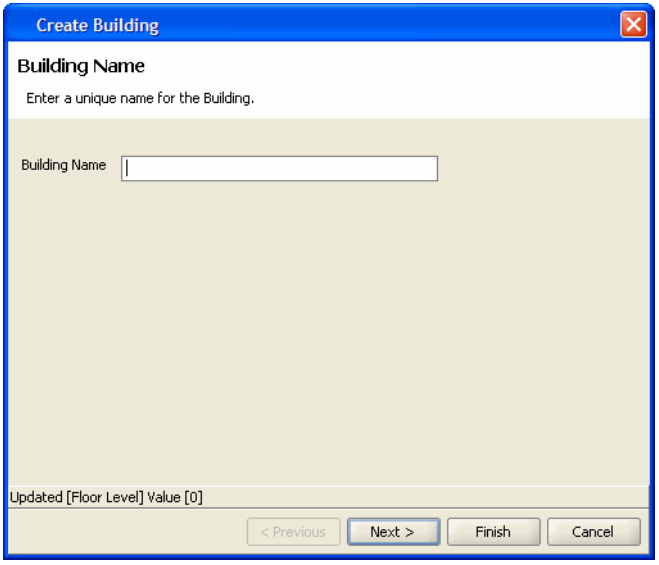
6 In the Channel Set (802.11b/g) list, select the set of operating channels for any 802.11b/g AP radios you plan to use (if different from the default), and click **Next**.

7 In the Number Of Buildings box, specify how many buildings are in your site, and click **Finish**.

When you specify the number of buildings a site contains, WLAN Management Software creates each building using the default settings. You can edit the buildings WLAN Management Software creates or you can add new buildings.

To create a building

1. In the Organizer panel, click the site name.
2. Select Create Building in the Task List panel. The Create Building wizard prompts you for information about the new building.

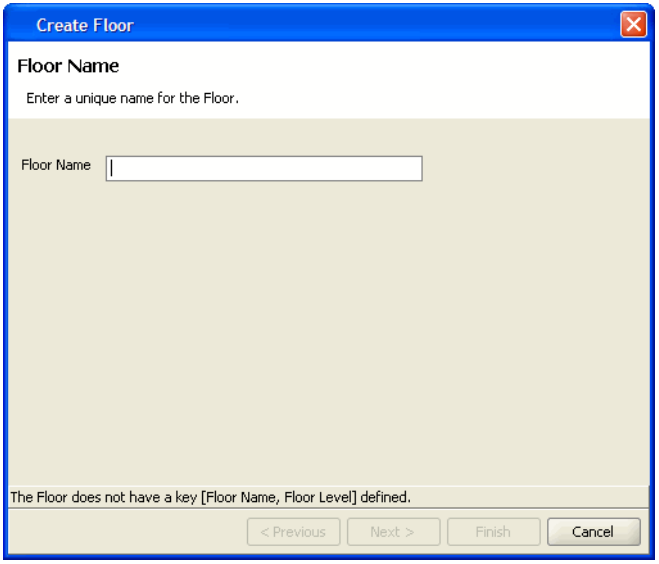


3. In the Building Name box, type the name of the building (1 to 30 alphanumeric characters, with no spaces or tabs), and click **Next**.
4. In the Number Of Floors box, specify how many floors the building has.

   When you specify the number of floors a building contains, WLAN Management Software creates each floor using the default settings. You can edit the floors WLAN Management Software creates or you can add new floors.
5. In the Starting Floor Level box, specify the floor number of the first floor in the building. To start with a subterranean floor, you can specify 0 or a negative floor number.
6. In the Skip Floor Levels box, specify floor numbers you want to skip. Skipping floors is useful when you want to model only certain floors in a building. Use commas to separate the floor numbers in a list; for example: 1,3,7. Use a hyphen when entering a range; for example: 8-12.
7. Click **Finish** to close the wizard.

To add a floor to the building

1. In the Organizer panel, click the building name.
2. Select Create Floor in the Task List panel. The Create Floor wizard prompts you for information about the new floor.



3 In the Floor Name box, type the name of the floor (1 to 60 alphanumeric characters, with no spaces or tabs), and click **Next**.

4 To change the default attenuation for radios, type the number of dB in the 802.11a (dB) box or 802.11b/g (dB) box.

5 In the Height of the Ceiling box, type the number of feet or meters from the floor to the ceiling (1 to 1000 feet or meters).

6 Click **Finish** to close the wizard.

Import a Floor Plan

Import existing floor plans into WMS. The file can be in one of the AutoCAD DXF, AutoCAD DWG, JPEG, or GIF formats.

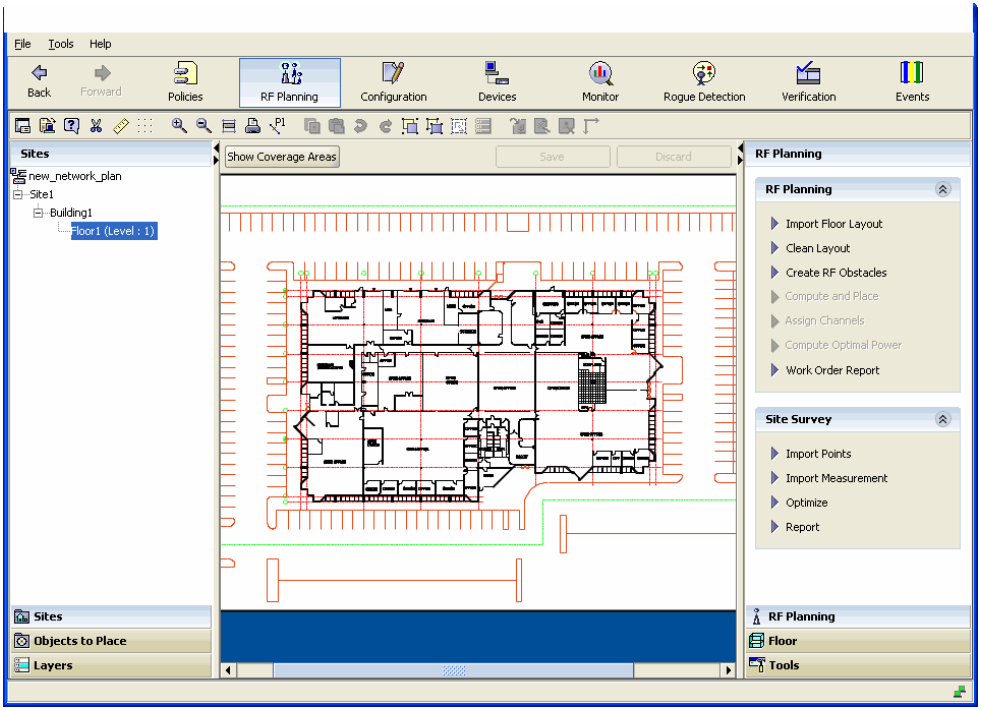
Note. Nortel recommends that you modify the AutoCAD files from AutoCAD to remove unnecessary objects and layers; then save them in .dxf format. For more information about how to modify AutoCAD files, refer to "Prepare the Floor Drawings" on page 130.

To import a floor drawing

1 In the Organizer panel, click on the plus sign next to the building to expand it, then click on the name of the floor for which you are importing the drawing. An empty floor layout appears in the Content panel.

2 In the Task List panel, under RF Planning, select Import Floor Layout. Browse to the file you wish to import, then click **Finish**. The imported drawing is displayed in the Content panel.

Figure 1: Floor Plan After Importing

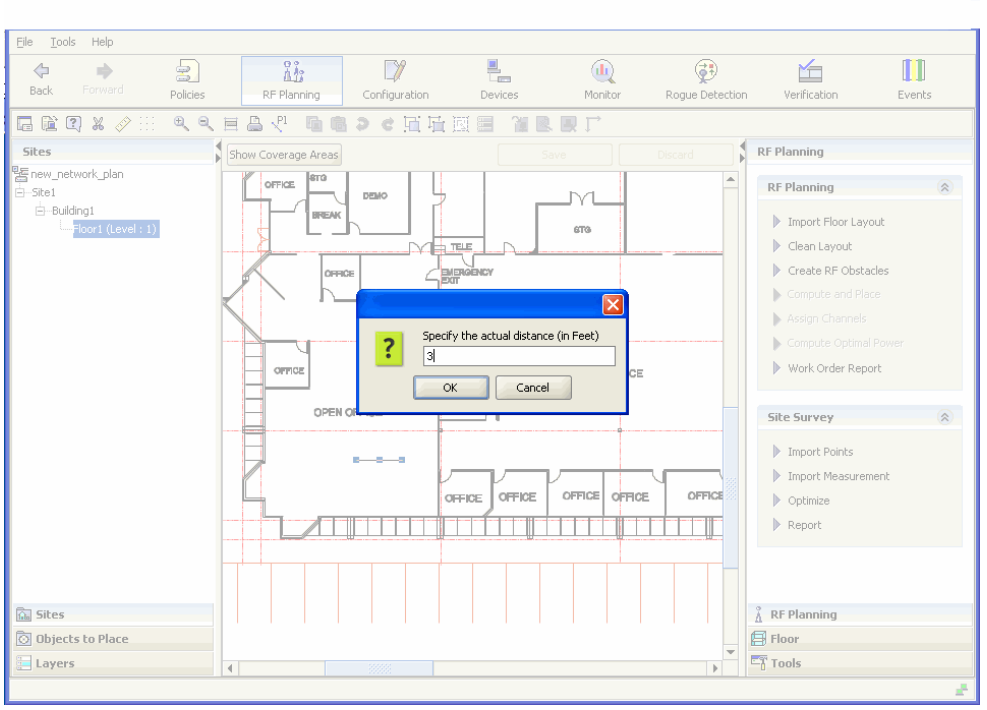


Set the Scale

Set the scale on your floor plan to better define the distance between objects in your network.

To set the scale

1. Display the floor plan in the Content panel.
2. Click on the toolbar.
   a. Draw a line on the floor plan over an object whose length you know; for example, a 3-foot door.
   b. Enter the actual length of the object in the pop-up box.
   c. Click **OK**.



Note. Zooming in on the object makes it easier to set the scale.

Clean Layout

Clean up your floor drawings further if unnecessary objects still remain after you perform an initial floor drawing cleanup.

Note the following when cleaning up a drawing:

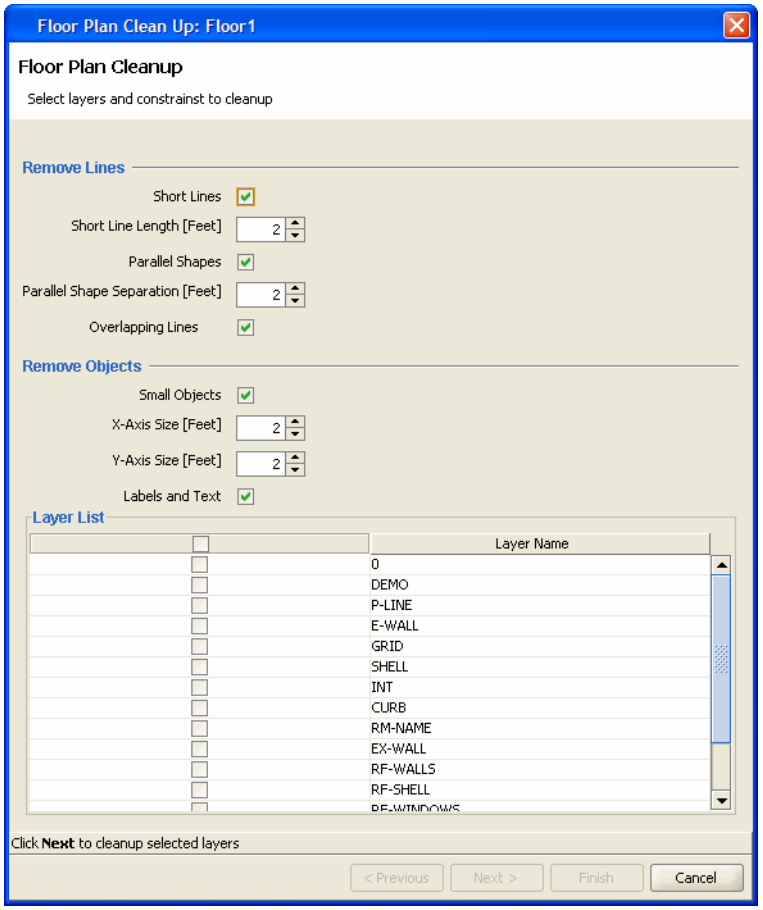
- Drawing cleanup does not apply to GIF or JPEG drawings.
- Drawing cleanup does not change objects that are grouped.
- If two objects that would normally be cleaned (such as two parallel lines close together) exist on different layers, then neither object is removed.

For more information about cleaning up your floor plans, refer to "Prepare the Floor Drawings" on page 130.

To clean up a drawing

1 Display the floor plan in the Content panel.

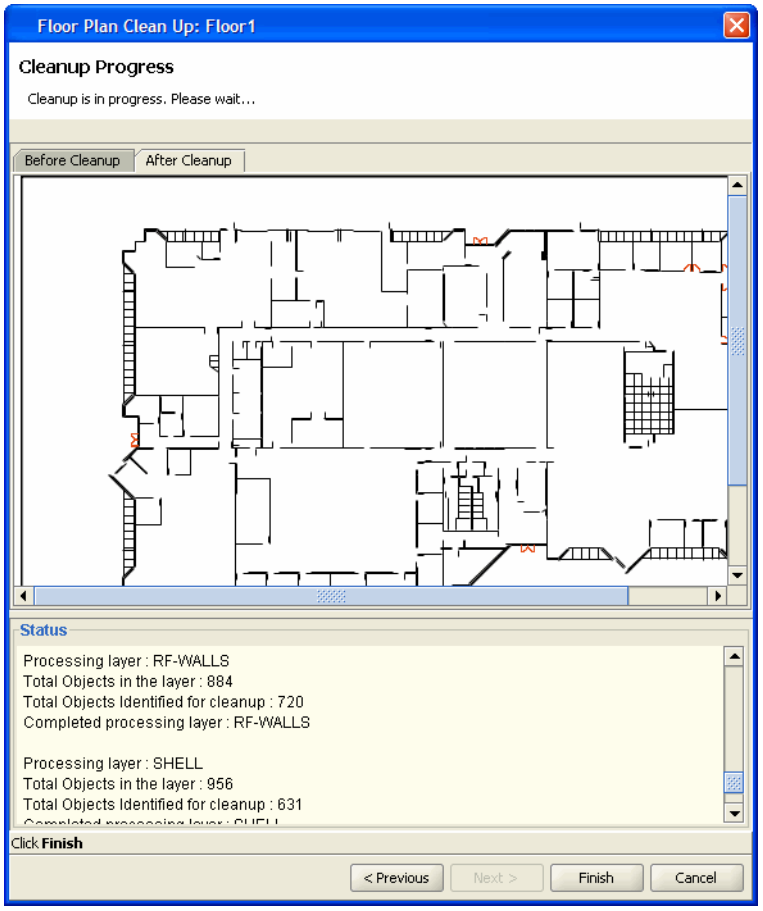
2 In the Task List panel, under RF Planning, click Clean Layout. The Floor Plan Clean Up wizard appears. Select the items you would like to remove from the floor plan. Select the layers you want to affect.



3 Click **Next**.

Cleanup progress is displayed at the bottom of the wizard.

4 You can display a Before Cleanup and After Cleanup view when cleanup is complete.



5 When you are satisfied with the results, click **Finish**.

Model RF Obstacles

When planning a Nortel network, consider how the building layout and physical objects affect signal loss. Walls, windows, and doors absorb RF signals, and different building materials have different attenuation factors.

You can model an RF obstacle on your floor plan and assign the obstacle type and attenuation factor, or assign an obstacle type and attenuation factor to objects in a DWG or DXF drawing. WMS uses these values when calculating coverage for the network.

If you do not have an imported drawing or if you are working with a GIF or JPEG image, create RF obstacles manually. If you are using an imported CAD drawing, convert many of the objects in the drawing into RF obstacles. All objects similar in construction material should be placed in one layer. For example, if the drawing file has walls in different

layers but after performing a site-survey the walls were found to be similar in material construction, it is better to put them in one layer. In this way, the RF attenuation assignment can be performed in one step.

This section shows how to select and draw objects and convert them into RF obstacles. WMS preserves the layers defined in a CAD drawing.

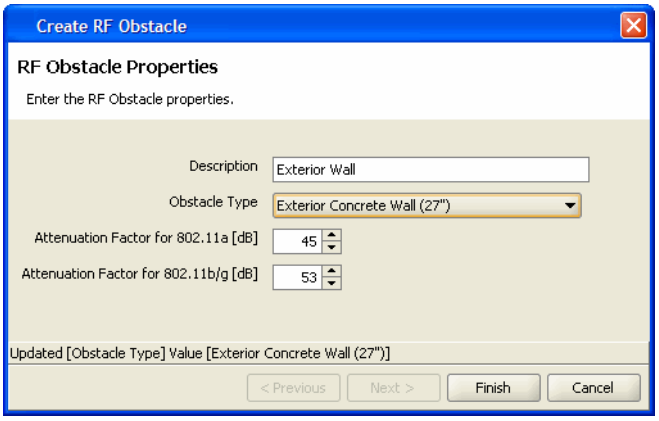
Table 1 provides some common AutoCAD layer terminology.

Table 1: Common AutoCAD Layer Terminology

AutoCAD Layer Name	Commonly Represents...
glaz	windows
scol	steel columns
p-fixt	bathroom
p-part	bathroom stall partitions
ext int	exterior interior

To create RF obstacles for all objects in a layer

1. Click Layers in the Organizer panel to bring up a list of the layers in the drawing.
2. Right-click one of the layers in the Organizer panel.
3. Select RF Obstacles under Create in the Task panel. The Create-Obstacle dialog box appears.



4. Define the RF obstacle.
5. Click **Finish**.

   The layer's objects are now obstacles in your floor plan.

Import a Site Survey

You can import RF measurement data by means of a site survey done outside of WMS. Using the Site Survey Order report from WMS, a map is created of your site that can be used in an Ekahau site survey. After the survey is complete, the measurement data can be imported back into WMS, and RF obstacles adjusted. In this way, actual, measured information about RF obstacles can be obtained and incorporated into your plan.

This guide contains post-deployment information about optimization on "Displaying the RF Coverage Area" on page 210. For pre-deployment information about optimization, refer to "Optimizing a Network Plan" in the *Nortel WMS Reference Manual.*

Plan RF Coverage

How you plan the RF coverage for your network depends on whether you are planning for the widest coverage or if you are planning for capacity. There are other contributing factors. One group of users might be mobile and require high throughput performance (a higher bandwidth), while another group of users are more stationary and require less throughput.

Select the **RF Coverage** tab in the Create Building wizard to define your coverage area. This section contains the following coverage tasks:

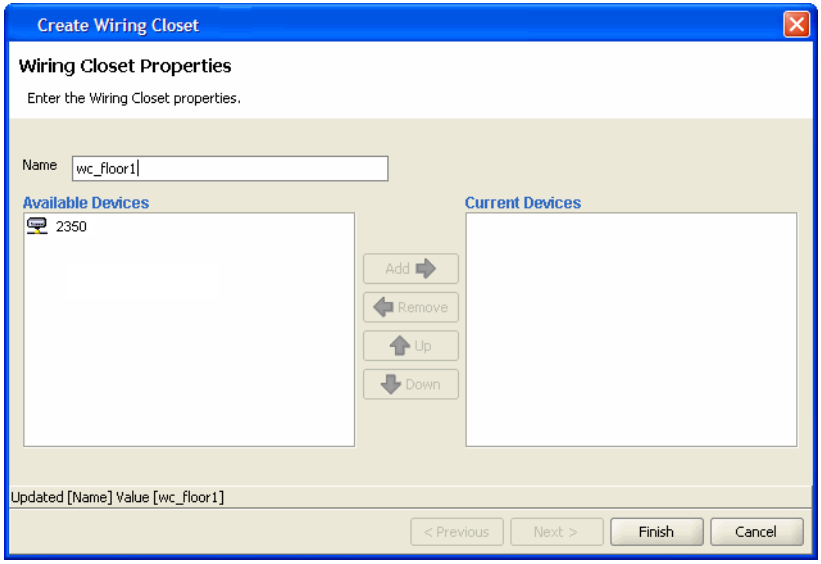
- "Add Wiring Closets" on page 143
- "Create Coverage Areas" on page 144
- "Compute and Place APs" on page 151
- "Assign Channel Settings" on page 154
- "Calculate Optimal Power" on page 155
- "Display Coverage" on page 156

Add Wiring Closets

A wiring closet is a container for switches. You need to add at least one wiring closet location to the floor plan. Also consider if you are installing direct APs. Direct APs (access points directly connected to the WSS) should be connected to the WSS with UTP Cat 5 cabling. The distance between the AP and the WSS in the wiring closet can not exceed 100 meters (330 feet).

To add a wiring closet

1. Display the floor plan in the Content panel.
2. In the Task List panel, click Tools.
3. In the Wiring Closer/Misc area under Coverage Area, click the Insert Wiring Closet icon.
4. Click in the floor display where you want to place the wiring closet. The Create Wiring Closet wizard appears.



5 In the Name box, type the name of the wiring closet (1 to 60 characters, with no tabs).

6 Click a WSS in the Available Devices box, then click the Add button to move it to the Current Devices box.

7 Click **Finish** to save the changes. The wiring closet is displayed on your floor plan.

Create Coverage Areas

The RF coverage area is the geographical area in your network you define RF coverage. As you configure the RF coverage area, consider the amount of bandwidth required for the area, as well as the number of users. You define the coverage area graphically on your floor plan using the coverage area drawing tool. Almost all shapes for a coverage area are possible. However, the following restrictions apply:

- A shape where two sides intersect each other is not permitted.
- A shared coverage area where there is a partial intersection is not supported.

WMS supports the sharing of coverage areas if one area is completely within a larger area. For example, you might want to provide 802.11a and 802.11b coverage in a conference room that is part of a larger coverage area only providing 802.11a coverage. AP are shared only in the overlapped area.

Note. When you draw a coverage area, it aligns to the grid to provide a whole number for width and height of the shape.

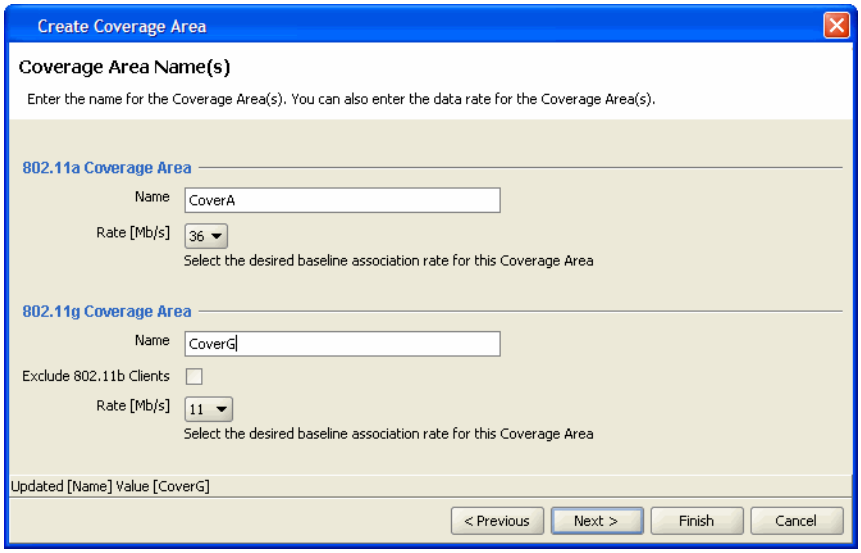
To create a coverage area

1 Display the floor plan in the Content panel.

2 In the Task List panel, click Tools.

3 In the Create area under Coverage Area, click one of the icon and draw the RF coverage area you want to add to the floor by clicking and dragging the mouse. The Create Coverage Area wizard appears.

4 Select one or more technologies you want to use in the coverage area and click **Next**. The wizard presents properties and association pages for the technology you chose in step 3.



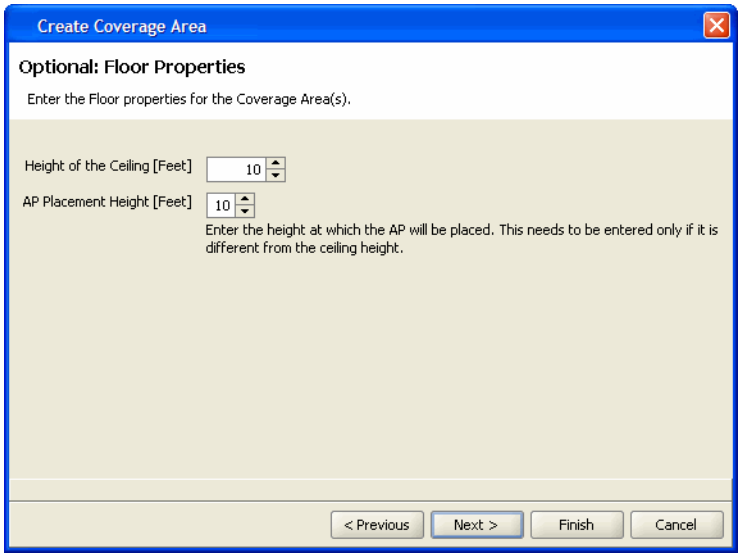
5 In the Name box for each technology, type a name for the coverage area (1 to 60 characters long, with no tabs).

6 In the Rate [Mb/s] list for each technology, select the average desired association rate for typical clients in this coverage area.

7 For 802.11g, to prevent the association of 802.11b clients to any radio in this coverage area, select **Exclude 802.11b clients**. To allow 802.11b clients to associate to radios in the coverage area, clear **Exclude 802.11b clients**.

Note. Even when association of 802.11b clients is disabled, if an 802.11b/g radio detects a beacon from an 802.11b network, the radio enters protection mode to protect against interference.

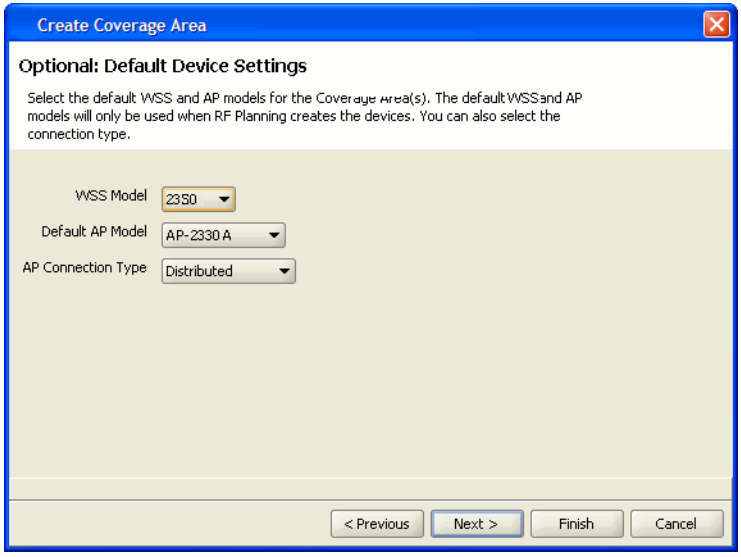
8 Click **Next**. The Floor Properties page appears.


Create Coverage Area
Optional: Floor Properties
Enter the Floor properties for the Coverage Area(s).
Height of the Ceiling [Feet]
10
AP Placement Height [Feet]
10
Enter the height at which the AP will be placed. This needs to be entered only if it is different from the ceiling height.
< Previous
Next >
Finish
Cancel

9 To change the ceiling height, specify the new height in the Height of the Ceiling box.

10 To change the height where APs are mounted, specify the new mounting height in the AP Placement Height box.

11 Click **Next**. The Default Device Settings page appears.


Create Coverage Area
Optional: Default Device Settings
Select the default WSS and AP models for the Coverage Area(s). The default WSS and AP models will only be used when RF Planning creates the devices. You can also select the connection type.
WSS Model
2350
Default AP Model
AP-2330 A
AP Connection Type
Distributed
< Previous
Next >
Finish
Cancel

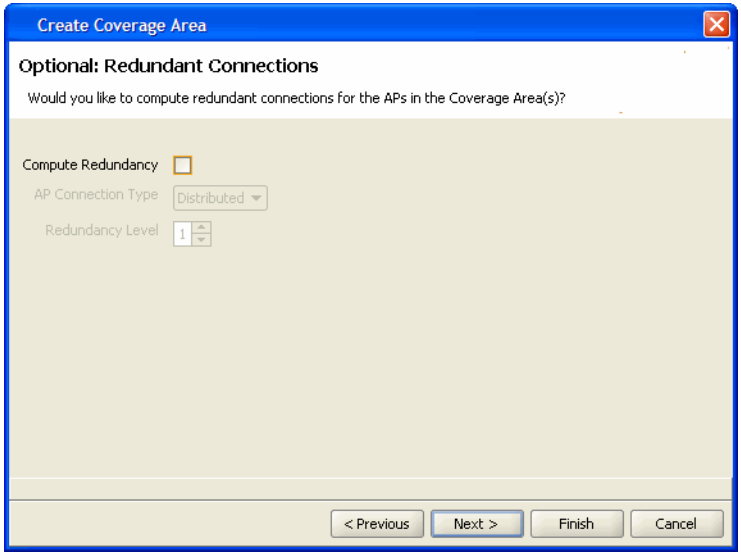
12 To change the default WSS model, select the model from the WSS Model list.

13 To change the default AP model, select the model from the Default AP Model list.

14 To change the AP connection type, select one of the following types from the AP Connection Type list:

- **Direct—APs are directly attached to dedicated WSS ports.**
- **Distributed—APs can be indirectly attached through intermediate Layer 2 or Layer 3 devices.**
- **Distributed (Auto)—APs can be indirectly attached through intermediate Layer 2 or Layer 3 devices. They receive their configuration automatically using a profile that assigns a Distributed AP number and name to the AP from among the unused valid AP numbers available on the switch.**

15 Click **Next**. If you selected Direct or Distributed in the AP Connection Type list, the Redundant Connections page appears; go to step 16. If you selected Distributed (Auto) in the AP Connection Type list, the Capacity Planning for Data page appears; go to step 20.



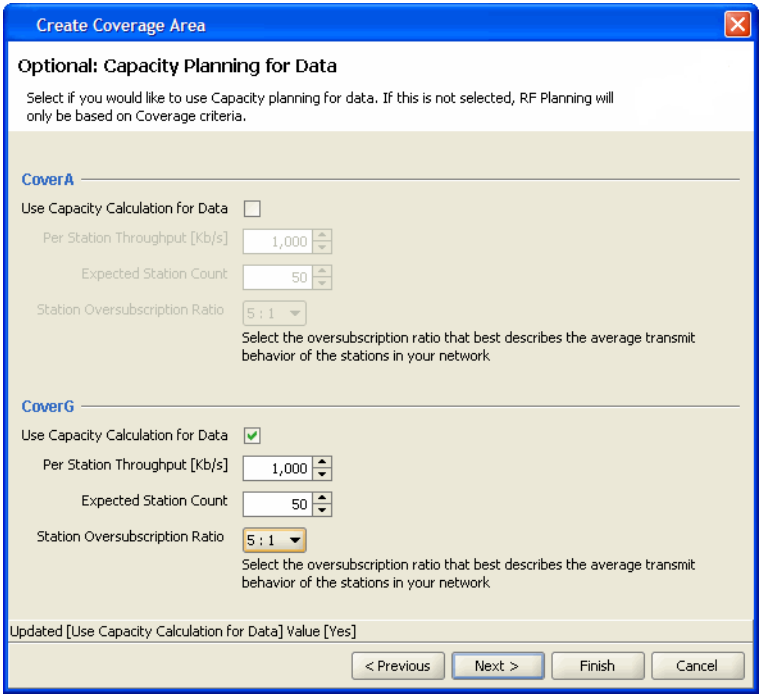
16 To plan for redundant AP connections to WSSs, select **Compute Redundancy**.

17 To change the AP connection type for the redundant connection, select **Direct** or **Distributed** from the AP Connection Type list.

18 To change the number of redundant connections for the distributed connection type, type the number in the Redundancy Level box.

For direct connections, the redundancy level is always 1.

19 Click **Next**. The Capacity Planning for Data page appears.


Create Coverage Area
Optional: Capacity Planning for Data
Select if you would like to use Capacity planning for data. If this is not selected, RF Planning will only be based on Coverage criteria.
CoverA
Use Capacity Calculation for Data
Per Station Throughput [Kb/s]
1,000
Expected Station Count
50
Station Oversubscription Ratio
5 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the stations in your network
CoverG
Use Capacity Calculation for Data
Per Station Throughput [Kb/s]
1,000
Expected Station Count
50
Station Oversubscription Ratio
5 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the stations in your network
Updated [Use Capacity Calculation for Data] Value [Yes]
< Previous
Next >
Finish
Cancel

20 To calculate AP placement and configuration based on both coverage and on capacity, enable **Use Capacity Calculation for Data**. Otherwise, click **Next** and go to step 24.

By default, WLAN Management Software performs only the coverage calculation. If you enable the **Use Capacity Calculation for Data** option, WLAN Management Software performs both calculations.

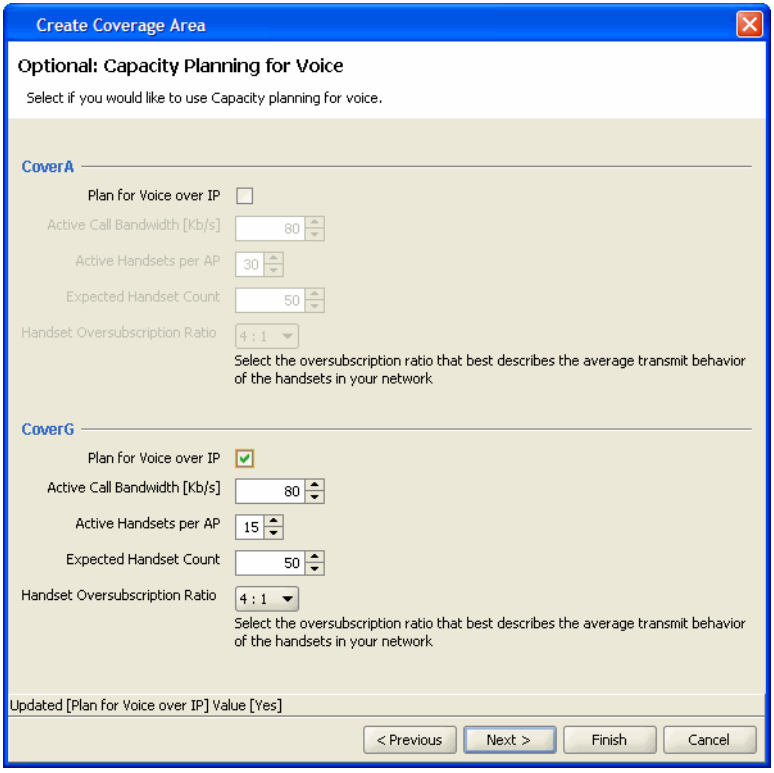
21 In the Per Station Throughput list, specify the throughput (combined transmit and receive) in kilobits per second (Kbps) for a station.

22 In the Expected Station Count list, specify the number of clients you expect to be in the coverage area.

23 In the Station Oversubscription Ratio list, select the ratio for the average transmit behavior of the stations.

The station oversubscription ratio is the ratio of active clients compared to total clients. For example, the ratio 5:1 indicates that, statistically, 20 percent of the clients are active at any given time.

24 Click **Next**. The Capacity Planning for Voice page appears.


Create Coverage Area
Optional: Capacity Planning for Voice
Select if you would like to use Capacity planning for voice.
CoverA
Plan for Voice over IP
Active Call Bandwidth [Kb/s]
80
Active Handsets per AP
30
Expected Handset Count
50
Handset Oversubscription Ratio
4 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the handsets in your network
CoverG
Plan for Voice over IP
Active Call Bandwidth [Kb/s]
80
Active Handsets per AP
15
Expected Handset Count
50
Handset Oversubscription Ratio
4 : 1
Select the oversubscription ratio that best describes the average transmit behavior of the handsets in your network
Updated [Plan for Voice over IP] Value [Yes]
< Previous
Next >
Finish
Cancel

25 To calculate AP placement and configuration based on both coverage and on capacity for voice over IP, enable **Plan for Voice over IP**. Otherwise, click **Next** and go to step 30.

By default, WLAN Management Software performs only the coverage calculation. If you enable the **Plan for Voice over IP** option, WLAN Management Software performs both calculations.

26 In the Active Call Bandwidth list, specify the amount of bandwidth in kilobits per second (Kbps) that you expect for each call.

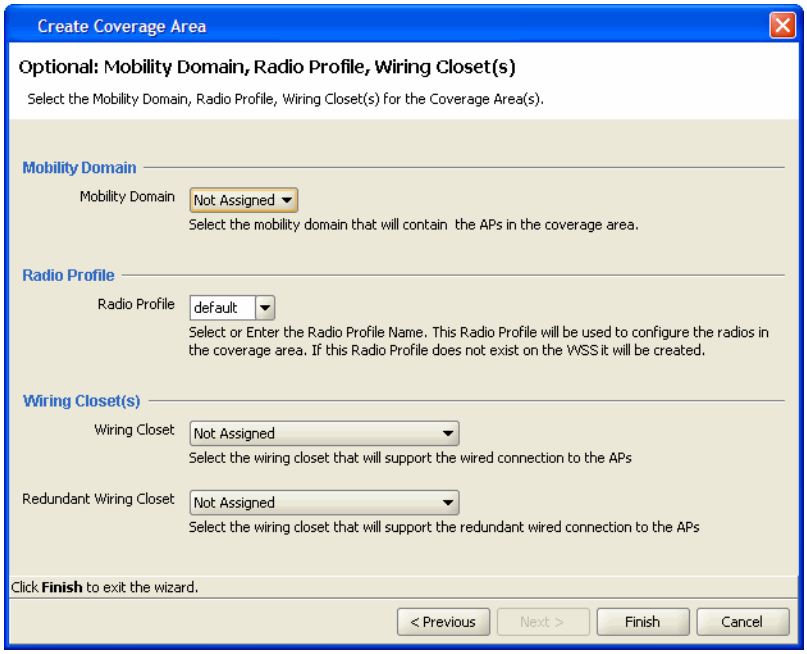
27 In the Active Handsets per AP list, specify the number of voice over IP phones that you want each AP to handle.

28 In the Expected Handset Count list, specify the number of voice over IP phones you expect to be in the coverage area.

29 In the Handset Oversubscription Ratio list, select the ratio for the average transmit behavior of the voice over IP phones.

The handset oversubscription ratio is the ratio of active handsets compared to total handsets. For example, the ratio 4:1 indicates that, statistically, 25 percent of the voice over IP phones are active at any given time.

30 Click **Next**. The Mobility Domain, Radio Profile, Wiring Closet(s) page appears.


Create Coverage Area
Optional: Mobility Domain, Radio Profile, Wiring Closet(s)
Select the Mobility Domain, Radio Profile, Wiring Closet(s) for the Coverage Area(s).
Mobility Domain
Mobility Domain
Not Assigned
Select the mobility domain that will contain the APs in the coverage area.
Radio Profile
Radio Profile
default
Select or Enter the Radio Profile Name. This Radio Profile will be used to configure the radios in the coverage area. If this Radio Profile does not exist on the WSS it will be created.
Wiring Closet(s)
Wiring Closet
Not Assigned
Select the wiring closet that will support the wired connection to the APs
Redundant Wiring Closet
Not Assigned
Select the wiring closet that will support the redundant wired connection to the APs
Click Finish to exit the wizard.
< Previous
Next >
Finish
Cancel

31 In the Mobility Domain list, select the Mobility Domain that contains the APs used for this coverage area.

32 In the Radio Profile list, select the radio profile used for this coverage area.

The profiles available depend on the Mobility Domain you selected in step 31. The profile you select applies to all radios associated with the coverage area. If you type the name of a radio profile that does not already exist, WLAN Management Software creates it.

33 In the Wiring Closet list, select the wiring closet that contains the WSS or switches to be connected to the shared AP.

If the APs will be directly connected to WSSs, a wiring closet is required. If all the APs in the coverage area will be indirectly connected to WSSs through the network, a wiring closet is not required.

34 In the Redundant Wiring Closet list, select the wiring closet that will provide redundant connection to the AP. This is required for directly connected APs, if you require the APs to have redundant connections. Otherwise, this is not required.

35 Click **Finish** to complete the wizard and create the coverage area. The coverage area is now displayed on your floor.

Compute and Place APs

When you perform the Compute and Place procedure for one or more coverage areas, WMS automatically calculates the number of AP you require and places them in appropriate locations on the floor. To do this, two calculations are performed in WMS. One is based on capacity (traffic engineering) and the other is based on pure RF coverage (at a given data rate).

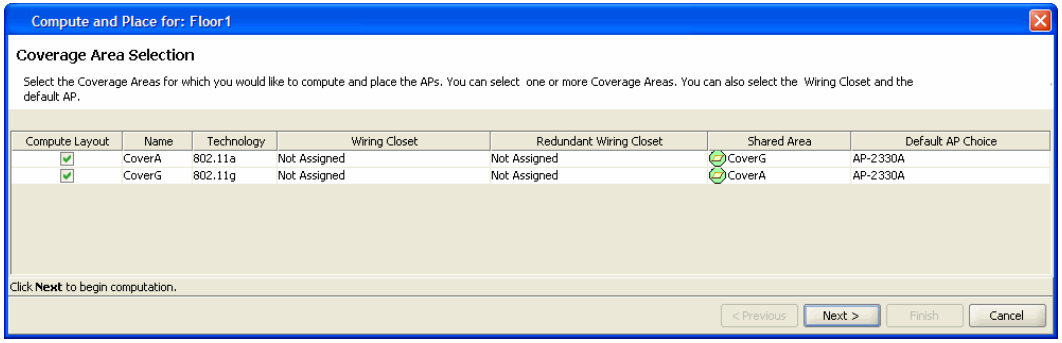
After the calculations are performed, the number of APs from capacity and the number of APs from coverage are compared, and the bigger count "wins." If capacity wins, a grid pattern of APs is established. The AP coverage positions are reused, with the excess APs remaining in their original grid position.

Note. Using a "clean" RF model is imperative for best results. If you have many parallel RF obstacles that are close together, the placement algorithm tends to add more APs than are required. So, even with the automatic clean layout mechanism in WMS, complex drawings demand additional pruning and isolation of single RF obstacles objects to keep the RF obstacle count as low as possible. For more information about cleaning your floor plans, refer to "Clean Layout" on page 138.

When you are performing Compute and Place for a coverage area for the first time, the results do not account for existing AP. Manual overrides of the AP results are not taken into account if you perform Compute and Place again.

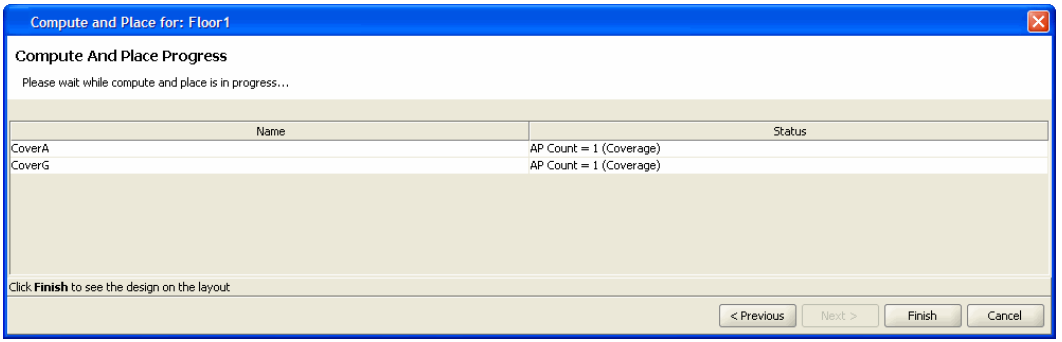
To determine the number and placement of APs

1. Display the floor plan in the Content panel.
2. In the Task List panel, click RF Planning.
3. Under RF Planning, click Compute and Place. The Compute and Place wizard appears.



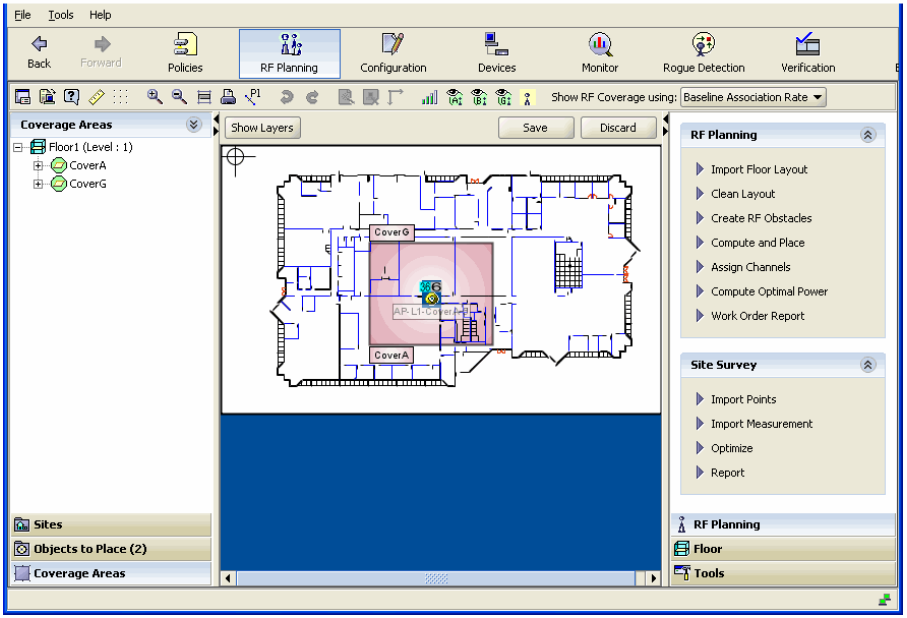
4. To remove a coverage area from AP placement and computation, clear the area's Compute Layout box.
5. To specify the primary wiring closet for a coverage area, click in the Wiring Closet column to display the wiring closet list and select a wiring closet from the list.

6 Click **Next**. The Coverage Area Progress page appears. Information is shown about the number of APs per coverage area, and whether they were placed based on coverage or capacity.



7 Review the number of AP required for each coverage area, and the overriding criterion used (coverage or capacity).

8 Click **Finish** to apply the changes. Icons for the suggested AP locations appear on the floor plan.

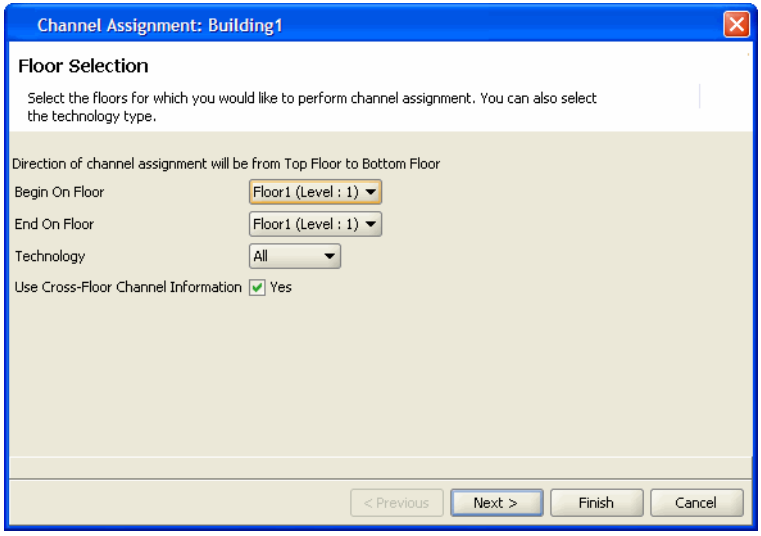


Assign Channel Settings

After identifying the AP required for a coverage area, you need to assign channels to the AP. Appropriate assignment of channels across the floor minimizes co-channel interference. The channel assignment algorithm assigns non-overlapping channels to neighboring APs from the selected channel set. Choose the starting floor and the ending floor (in the downward direction) for multi-floor channel assignment. The algorithm takes predicted RSSI values between neighboring APs (including APs on different floors and 3rd party APs) and minimizes same-channel assignments between APs. You can specify cross-floor attenuation and the 802.11 technology on which you want to perform the channel assignment. WMS uses predicted RSSI values for the imaginary "ray" that is drawn between two APs. Consequently, you might see unexpected results if the exact path between the APs has many obstacles, but the areas around that path are relatively open. You can make further manual adjustments, if necessary.

To assign channels

1. Display the floor plan in the Content panel.
2. In the Task List panel, click RF Planning.
3. Under RF Planning, click Assign Channels. The Channel Assignment wizard appears, showing the current channel assignment constraints.


Channel Assignment: Building1
Floor Selection
Select the floors for which you would like to perform channel assignment. You can also select the technology type.
Direction of channel assignment will be from Top Floor to Bottom Floor
Begin On Floor
Floor1 (Level : 1)
End On Floor
Floor1 (Level : 1)
Technology
All
Use Cross-Floor Channel Information
Yes
< Previous
Next >
Finish
Cancel

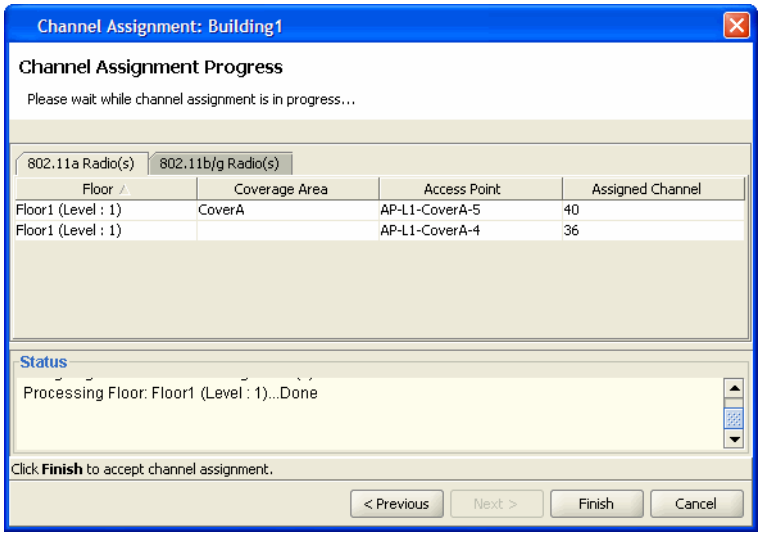
4. To change the starting floor for channel assignment, select the floor from the Begin On Floor List. By default, WLAN Management Software starts at the top floor and works down.
5. To change the ending floor for channel assignment, select the floor from the End On Floor List.

   The ending floor number must be lower than or equal to the starting floor number.
6. To change the radio type for which to assign channels, select the radio type from the Technology list. By default, WLAN Management Software assigns channels for all radio types on the AP placed in the building.

7 To prevent WLAN Management Software from taking the channel assignments for the floor above into account when calculating the channel assignments for a floor, clear **Use Cross-Floor Channel Information**.

8 Click **Next**. The Channel Assignment Progress page appears.

9 Review the results. The 802.11a channel assignments are listed on the 802.11a Radio(s) tab. The 802.11b/g channel assignments are listed on the 802.11b/g Radio(s) tab.



10 Click **Finish** to accept the channel assignments.

The new channel assignments are reflected in the Coverage Areas panel.

Calculate Optimal Power

The Compute and Place procedure is performed using the maximum allowed power for the selected channel set in the defined regulatory domain. Optimal power can be computed for each AP, where transmit power is adjusted (up or down) to provide adequate coverage with minimum RF interference.

When calculating optimal power, you can manually change positions and counts of APs (add or remove APs) before the final power optimization is performed. Changing AP quantities and positions is quite typical, given that an operator can interpret the floor plan and understand any cabling constraints to avoid any positioning problems.

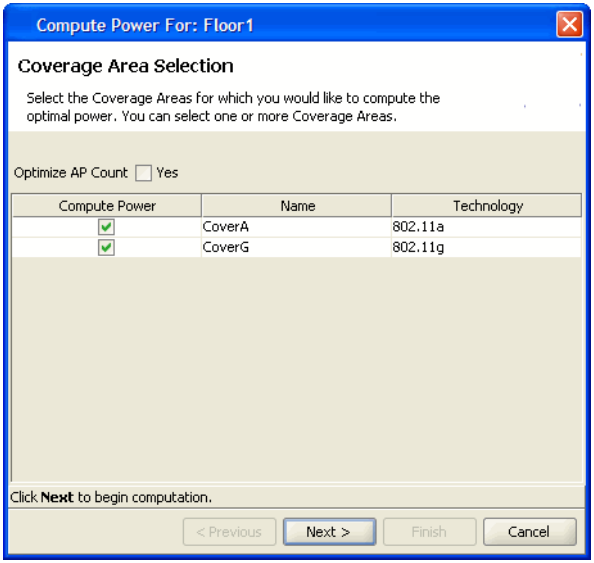
Transmit power levels must be high enough to adequately cover an area, but also low enough to minimize co-channel interference. WMS factors in these considerations when calculating optimal power.

To calculate optimal power

1 In the Task List panel, click RF Planning.

2 Under RF Planning, click Compute Optimal Power.

The Compute Power For wizard appears, showing a list of the areas you defined and the corresponding technology.



3. To optimize the AP count, select **Optimize AP Count**. This option checks for coverage overlaps and removes an AP if neighboring APs provide enough coverage to make the AP unnecessary.
4. Select **Compute Power** for the areas for which you want to compute power.
5. Click **Next**. The Compute Power For Progress page appears. Click **Finish** to view the results.

Display Coverage

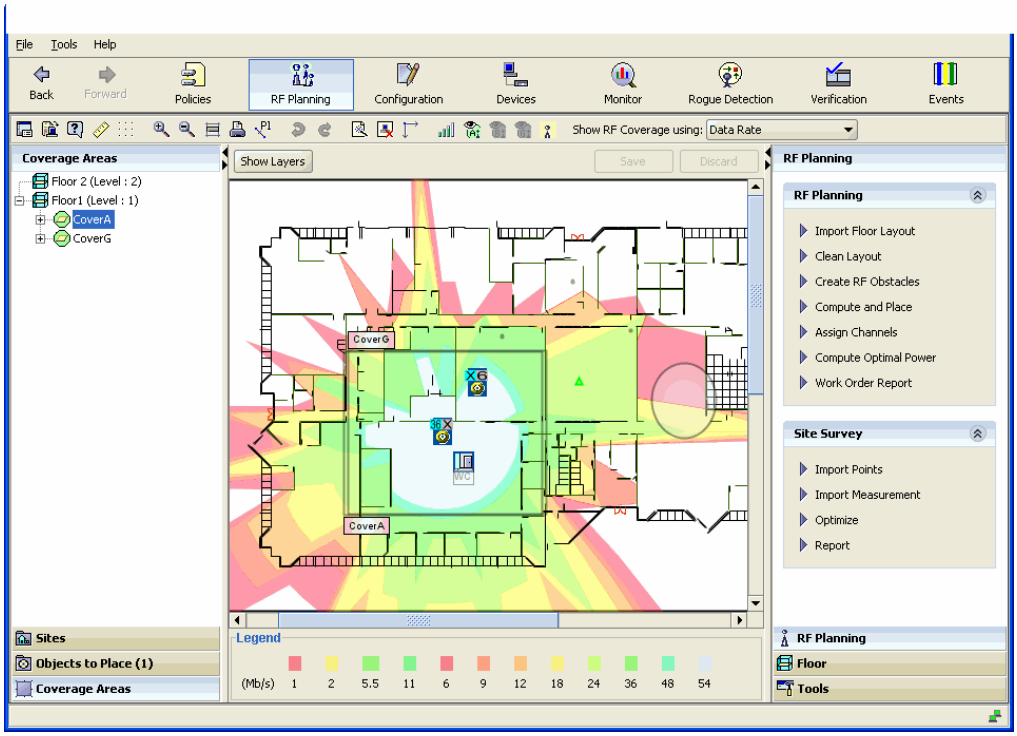
Looking at the RF coverage allows you to see if the entire area is adequately covered by the AP. You can move the APs and see how the coverage changes.

To display the RF coverage for an area

1. Beside **Show RF Coverage Using**, select how you want to display the coverage.
   - **Baseline Association Rate—Coverage is shown based on the AP radio baseline association rate. The baseline association rate is the typical data rate the radio is expected to support for client associations. (The baseline association rate is specified during planning, on a coverage area basis.)**
   - **Data Rate—Coverage is shown in colored bands that represent each of the data transmit rates supported by the radio. These rates are standard for each radio type.**
   - **RSSI—Coverage is shown based on the received signal strength indication (RSSI) of the radio's signal heard by other radios.**
2. Right-click on a coverage area and select **Show RF Coverage**.

3 Select the **A**, **B**, or **G** icon from the toolbar to view the coverage area for that technology.

The coverage area is displayed, color-coded by channel.



If the coverage area provided by an AP on the floor above or below is one meter or less, WLAN Management Software displays a message. This coverage area is not displayed on the floor plan.

Generate a Work Order

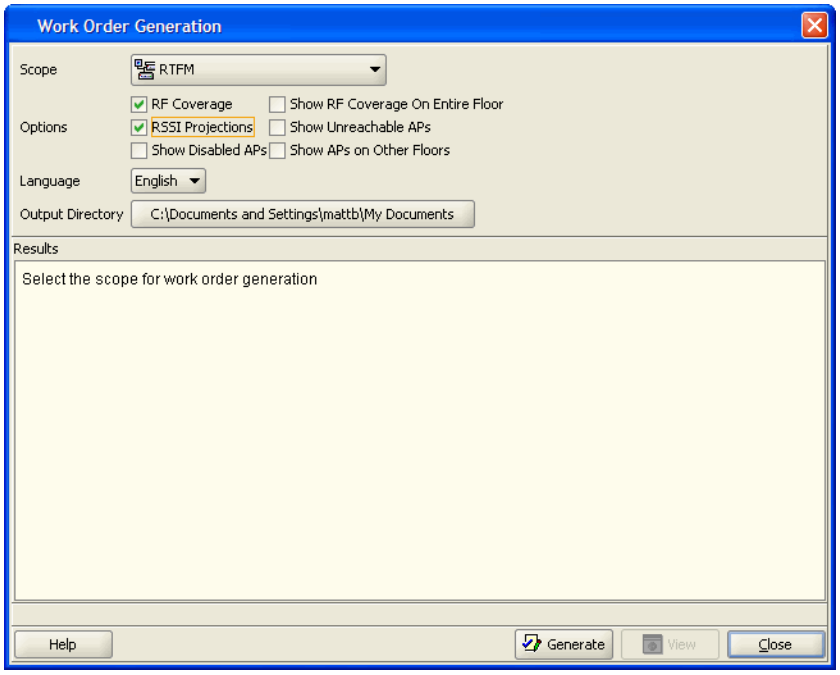
You can generate a work order as part of your wireless network planning. The work order provides all of the necessary information for the physical installation of the Nortel WLAN 2300 System. A work order shows where the AP should be installed, WSS initial setup configuration information, and projected RSSI information that is useful when verifying the installation.

To generate a work order

1 Display the floor plan in the Content panel.

2 In the Task List panel, click RF Planning.

3 Under RF Planning, click Work Order Report. The Work Order Generation dialog is displayed.



4 Specify the work order options.

5 In the Language list, select **English** or **German**.

The language you select is the language used when you next access this page.

6 To select the directory to which the work order report is saved, click **Choose**. The **Select** dialog box appears.

For Linux systems, the default directory is the home directory of the user running WMS.

7 Click **Generate**.

The work order is saved in the directory you specified in the format WO_*scope_name_date*. If you generate another order for the same scope on the same day, the old work order is overwritten.

8 Click the link in the Results area of the dialog. A browser window opens to display the work order in HTML format.

Install the Equipment

After you print the work order from WMS, you can distribute it to your installers. The work order shows where to install the Nortel equipment. If you have specified third-party APs in the network plan, those will be considered in the work order, too.

For more information about installing the equipment, refer to "Equipment Installation" on page 46.

What's Next?

A WMS network plan can support both Auto-RF and RF Planning techniques at the same time. You can use Auto-RF to meet the demands of rapid network changes that can be caused by a greater or lesser number of users, or by a physical blockage of APs. You are alerted when changes occur in your network of this nature.

- To fine tune your network's RF coverage area and performance, refer to "Optimizing a Network Plan" on page 201.
- To deploy your network plan and enable and configure monitoring, refer to "Managing and Monitoring Your Network" on page 161

Managing and Monitoring Your Network

What Is Network Management? 161
What Is Network Monitoring? 161
Deploy Your Configuration 162
Perform Basic Administrative Tasks 163
Distribute System Images 164
Import and Export Switch Configuration Files 167
Monitoring Examples 168
What's Next? 182

What Is Network Management?

This chapter provides information to help you deploy the services you configured for your wireless network, enable communication between a WMS client and WLAN Management Software Services, and enable and configure monitoring. It also provides you with information about configuring WSS management services and performing specific administrative tasks.

For detailed information about performing administrative tasks on a WSS, refer to the "Configuring WSS System and Administrative Parameters" chapter in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

What Is Network Monitoring?

In addition to management capabilities, this chapter highlights the Monitor function, which displays information retrieved from the WMS service. The Monitor views show correlated data and allow you to navigate to the details. Information is presented in the following views under the Monitor tool bar option:

- Status Summary—Shows the high-level status for Nortel equipment.
- Client Summary—Shows activity, errors, and session information for network clients. You can also manage RF Link Test.
- Alarm Summary—Shows faults (alarms) for WSSs.
- Traffic Summary—Shows traffic statistics for the network and monitors the traffic views.

Clicking the **Details** button in any of the previous views provides more information about the data in that view.

Once you are familiar with the Monitor function, this chapter also provides three monitoring examples you can use as a guide to troubleshooting user connectivity issues in your network

For detailed information about monitoring, refer to the "Monitoring the Network" chapter in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

The RF analysis function analyzes RF statistics and the RF Visualize function uses 3D RF mapping to improve RF modeling and service location.

Deploy Your Configuration

Any changes you make to your network in WMS are saved in the network plan on the server, but the changes are not applied to the network until they are deployed. You see the changes in WMS, but the changes are only in the network plan. To implement the changes in the live network, you must deploy them to the WSSs in the network. You can easily apply a configuration to multiple WSSs, or deploy changes to a single WSS.

WLAN Management Software allows you to deploy changes immediately or schedule deployment of the changes.

To immediately deploy local changes

1. Select the Devices tool bar option.
2. At the bottom of the Task List panel, select Change Management.
3. Select one or more WSSs.

   To select multiple switches, press **Shift** (for contiguous switches) or **Control** (for noncontiguous switches) while clicking.
4. In the Local Changes group in the Task List panel, click **Deploy**. The Deploy Configurations dialog box appears.

   The dialog lists the switches that have configuration changes.
5. Select the switches to which you want to deploy the changes.

   To select more than one WSS, click **Shift** while clicking to select contiguous items, or click **Ctrl** while clicking to select noncontiguous items.
6. Click **Deploy**.

   The deployment status for each affected WSS is shown in the History window at the bottom left of the dialog box.

   WLAN Management Software performs verification of the changes. If errors occur, they are listed in the Selected Errors at the bottom right of the dialog box. If there are errors, fix them and verify the changes before trying to deploy again. (You can use the Verification tab to fix the errors.)

   If the deploy is successful, WMS also instructs the WSS to save the changes in its configuration file.
7. Click **Close**.

Note. You can click **Close** at any time after clicking **Deploy**. The operation continues in the background. To review the status of the operation, use the operation log. (Select View Operation Log in the Task List panel.)

To schedule deployment of local changes

1. Select the Devices tool bar option.
2. At the bottom of the Task List panel, select Change Management.
3. Select one or more WSSs.

   To select multiple switches, press **Shift** (for contiguous switches) or **Control** (for noncontiguous switches) while clicking.
4. In the Task List panel in the Local Changes group, click **Schedule Deploy**. The Schedule Deploy dialog box appears.
5. Edit the start date and time (The date and time are based on the date and time on the machine where WMS Services is installed.
6. Click **OK**.

To verify your deployment

1. Leave the Devices tool bar option selected.
2. Look in the Deploy Status column for the switch(es) to which you deployed configuration information. The status should be *Deploy Completed*.

You also can verify successful deployment by checking the operation log.

To access the log

1. Select the Devices tool bar option.
2. At the bottom of the Task List panel, select Device Operations.
3. In the Task List panel, select View Operation Log.

Perform Basic Administrative Tasks

This section contains information about basic administrative tasks you can perform in WMS.

For detailed information about performing administrative tasks including configuring WSS management services, see the chapter “Configuring WSS System and Administrative Parameters” in the *Nortel WLAN Management Software 2300 Series Reference Guide*.

For more information about image and file management, see the chapter “Managing WSS System Images and Configurations” in the *Nortel WLAN 2300 System Software Command Line Reference*.

Configuring WSS Management Services

You can configure the following information and management services for the WSS:

- System information—You can specify system contact information, as well as the CLI prompt and the banner message that appears at each session.

- HTTPS—By default, HTTPS is enabled. TCP port 443 is used for secure access by Web View, the Nortel Web-based application for managing a WSS.

Note. WMS communications also use HTTPS, but WMS is not affected by the HTTPS configuration on the WSS. For WMS, HTTPS is always enabled and listens to port 8889.

- Telnet—By default, Telnet is disabled. You can enable Telnet for unencrypted access to the CLI.
- SSH—By default, SSH is enabled. You can use SSH for encrypted access to the CLI.
- SNMP—By default, SNMP is disabled. You can configure SNMP community strings and User Security Model (USM) users, notification profiles, and notification targets.
- Logging—The system log provides event information for monitoring and troubleshooting. You can send the log information to a local data buffer on a WSS, to the console, to a Telnet session, and to a configured set of syslog servers.
- Tracing—Tracing allows you to review diagnostic information for debugging WSS Software. Tracing allows you to review messages about the status of a specific area of WSS Software.
- Time zone and summertime settings—You can configure the system time and date statically. You also can configure WSS Software to offset the time by an additional hour for daylight savings time or similar summertime period.

To manage services on a WSS

1. Select the Configuration tool bar option.
2. In the Organizer panel, click the plus sign next to the WSS.
3. Click the plus sign next to System.
4. Select Management Services. The management services and their settings appear in the Content panel.
5. Use the Content panel and Task List options to modify settings.

   (For information about the management options, see the "Viewing and Changing Management Settings" section in the "Configuring WSS System Parameters" chapter of the *Nortel WLAN Management Software 2300 Series Reference Guide*.)

Distribute System Images

You can use WLAN Management Software to upgrade or downgrade the system image (WSS Software software) on WSSs. System images include switch software and AP software.

Using the Image Repository

Use the image repository to add or delete WSS system images. The image file is checked and its version is verified when added to the image repository. Images are stored in the *WMS_installation_directory*\images\dp directory.

To add a system image

1. Select the Devices tool bar option.

2 At the bottom of the Task List panel, select Device Operations.

3 In the Task List panel, select Image Repository.

4 Click **Add Image**. The Add to Repository dialog box appears.

5 Navigate to the directory containing the system image.

6 Select the system image.

7 Click **Add to Repository**. The image is added to the image repository and appears in the Image List.

8 To close the Image Repository dialog box, click **Close**.

To delete a system image:

1 In the Image Repository dialog box, select the image you want to delete.

2 Click **Remove Image**. A prompt appears.

3 Click **Yes** to delete the system image.

4 To close the Image Repository dialog box, click **Close**.

Distributing System Images

You can distribute a system image to one or more WSSs in a network plan.

To use a new system image, you must reboot the WSS.

Note. Nortel recommends that you use the Verification tab to resolve any configuration errors or warnings before you distribute system images.

Note. Before you can distribute an image, you must add it to the image repository. (See "Using the Image Repository" on page 164.)

To immediately install an image on WSSs

1 Select the Devices tool bar option.

2 At the bottom of the Task List panel, select Device Operations.

3 In the Managed Devices list, select the WSSs onto which you want to install the image.

To select more than one WSS, click **Shift** while clicking to select contiguous items, or click **Ctrl** while clicking to select noncontiguous items.

4 In the Task List panel, select Image Install.

5 Click on Select an Image to display the list of images in the repository.

6 Select the image and click **Install**.

To schedule installation of an image on WSSs

1. Select the Devices tool bar option.
2. At the bottom of the Task List panel, select Device Operations.
3. In the Managed Devices list, select the WSSs onto which you want to install the image.

   To select more than one WSS, click **Shift** while clicking to select contiguous items, or click **Ctrl** while clicking to select noncontiguous items.
4. In the Task List panel, select Schedule Install.
5. Click on Select an Image to display the list of images in the repository.
6. Click **Next**.
7. Edit the start date and time.

   (The date and time are based on the date and time on the machine where WLAN Management Software Services is installed.)
8. Click **Finish**.

Saving Versions of Network Plans

You can save multiple versions of a network plan in WMS. After deploying a network plan to a WSS, you can save a snapshot of the plan as a version. Create versions of the network plan on a regular basis and at every major baseline event for network configurations. Doing so allows you to have snapshots of network configurations should you need to revert to one of them.

If you need to roll back configuration changes, you can use a saved version to roll back the system software image and configuration files to a known state. Before you can save a version of a network plan, you need to deploy and save the network plan. Versions of network plans are saved in the db/xml/versions directory in the WMS installation directory.

After you have saved a version of a network plan, the version appears in the list of network plans available to open. If you open a version of a network plan, you are asked whether you want to deploy it or open it. When the version is open, the version name is displayed in the title bar of the main WMS window.

To save a version of a network plan:

1. Select **Services > Plan Management**. The WLAN Management Software Services Plan Management page is displayed in a browser window.
2. In the left-hand column of the page, click Save As. The Save As Network Plan page is displayed.
3. In the Network Plan Name field, type a name for the plan. Make the name descriptive. For example, name the plan *Pleasanton_campus*.
4. Click **Save**.

Saving Network Plans Automatically

By default, WMS uses the autosave feature to automatically save changes to a network plan at regular intervals while you are working.

To view or modify backup settings, select **Services > Backup & Restore** to display the Backup & Restore page in a browser window.

Import and Export Switch Configuration Files

You can import or export switch configuration files in Extensible Markup Language (XML) format.

- The import option enables you to create a WSS in the network plan by importing configuration files in Extensible Markup Language (XML) format. You also can update the configuration of a switch that is already in the plan.
- The export option enables you to save a switch's configuration to an XML file. After exporting a WSS configuration to an XML file, you can import it to another instance of WMS or use it as a backup copy.

If you import a configuration containing information that an older version of WMS or WSS Software does not support, the information is ignored when the configuration is imported.

If you import a switch configuration, you must enable WMS management of the switch before you can deploy the switch to the network. (To enable WMS management of a switch, select the switch in the Organizer panel, select Managed, then click **Save**.)

To import a configuration:

1. Select **Tools > Import** in the main WMS window. The Import Configurations dialog box appears.
2. In the Import Into Mobility Domain group box, select one of the following options:
   - **Click Use File Info to import the configuration information using the Mobility Domain specified in the configuration file.**
   - **Click Select to specify a Mobility Domain to import configuration information to. Then select the Mobility Domain from the list.**
3. To replace existing WSS information in WMS with information from the configuration file, select **Update existing** WSSs.
4. Click **Select Files**. The Select Files To Import dialog box appears.
5. Select one or more configuration files to be imported. To make multiple selections, press **Shift** (for contiguous items) or **Control** (for noncontiguous items) while clicking items.
6. Click **Select Files To Import**. The file or files you selected appear in the File Import Results list.

   Click **Clear Files** to remove all the files you previously selected.
7. Click **Import**. The status of the import process appears in the Status column.
8. Click **Close** to save the changes.
9. Enable WLAN Management Software to manage the switch.
   a. To enable WLAN Management Software management of a switch, select the switch in the Organizer panel, select Managed Click **Save**.

To export a configuration

1. Select **Tools > Export**. The Export Configurations dialog box appears.
2. In the Export From/To list, select the Mobility Domain with the configuration you want to export.
3. Click the **Choose** button, which is labeled with the current output directory, to export the configuration file to a different directory. The Select dialog box appears. Navigate to the directory you want to use as the output directory, and click **Select**.

On Linux systems, the default directory is the home directory of the user running WMS.

4 Select **Overwrite Existing Files** to overwrite previously exported configuration files.

If you do not select this option, you cannot export a configuration file with the same name as an existing file in the output directory. You can rename the existing file or move the file to another directory.

5 Select **Copy Files Before Overwriting** to have WMS create a backup copy of a previous configuration file.

6 Select **Export Defaults** to include the default configuration commands in the exported file.

7 Ensure the **Export** checkbox is selected for each WSS whose configuration you want to export.

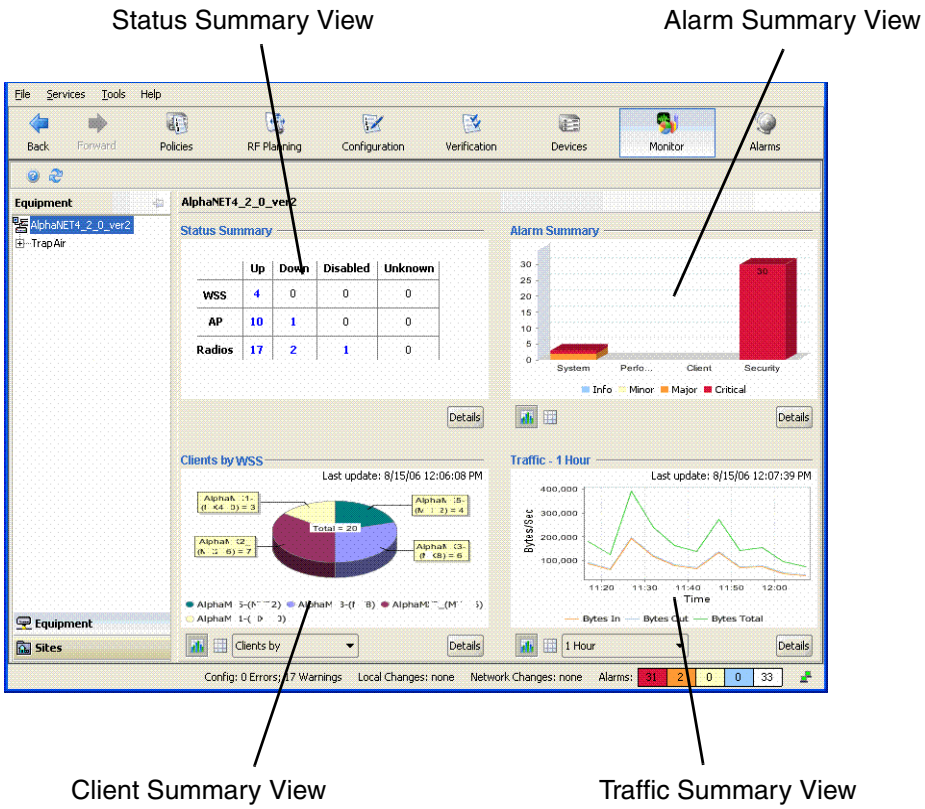
8 Click **Export** to begin the exporting process. Messages appear in the Status column in the WSS List box and the Results box. The configuration is saved in the directory that you specified.

9 To close the Export Configurations dialog box, click **Close**.

Monitoring Examples

When you click on the Monitor tool bar option. you will notice several different sections or *views*. Each view is a different way to examine data that WMS captures. The monitor dashboard includes the following views:

- Status Summary
- Alarm Summary
- Client Summary
- Traffic Summary



Each view provides answers to specific questions; for example, how many clients connected over the last hour, and which WSS has the most traffic load? The Alarms Summary, Clients, and Traffic sections provide buttons so that you can switch between graphical and tabular views in the same panel. These buttons allow you to see the data behind each graph.

WMS provides many monitoring options. This section describes how you can use some of the monitoring tools to determine problems that are typically reported to a network operator.

The monitoring examples described in this section are based on the following scenarios:

- An individual user calls the help desk with the complaint that the network is very slow or inaccessible
- A group of users complain about network performance

Monitor an Individual User

If an individual user notifies you that the network is very slow or inaccessible, perform the following steps to identify the problem:

1. Find the user in the list of users on the network.

2. Locate the user in the floor plan. (If you can locate them, then the scope of the problem can be narrowed down to performance.)
3. View the user's network activity.
4. View network performance statistics for the user's session.

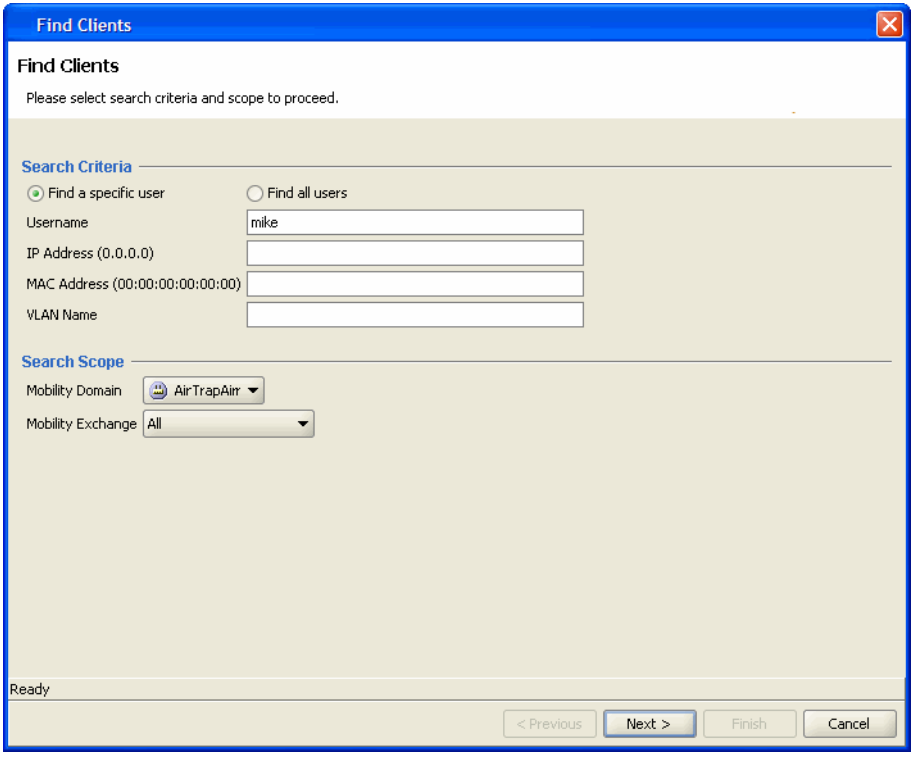
Find the User

You can find a user or multiple users based on the following criteria:

- Username
- IP address
- MAC address
- VLAN name

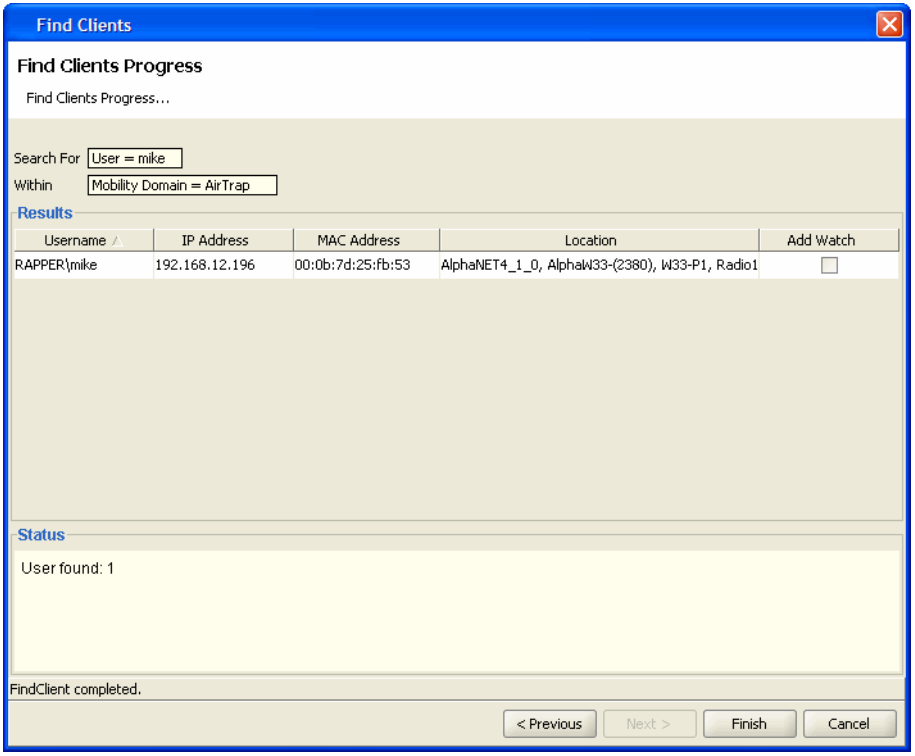
To find the user

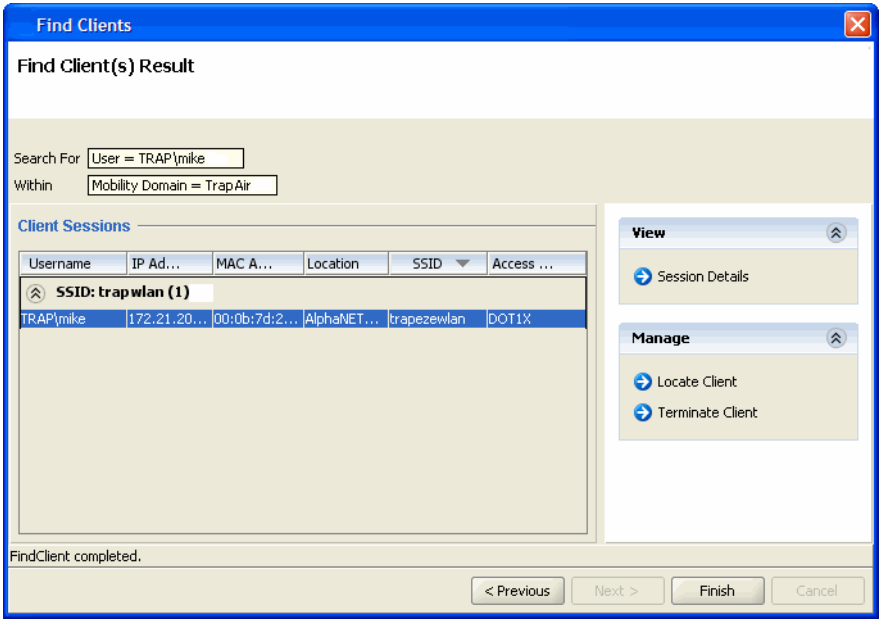
1. Click on the Monitor option in the main WMS tool bar.
2. Click **Details** in the Client Summary View to switch to the Client Monitor View.
3. Click Find Client under the Manage section of the Task panel. The Find Clients dialog box appears, as shown below.



4 Enter the desired search criteria, and select the search scope.

5 Click **Next**. The search results appear.





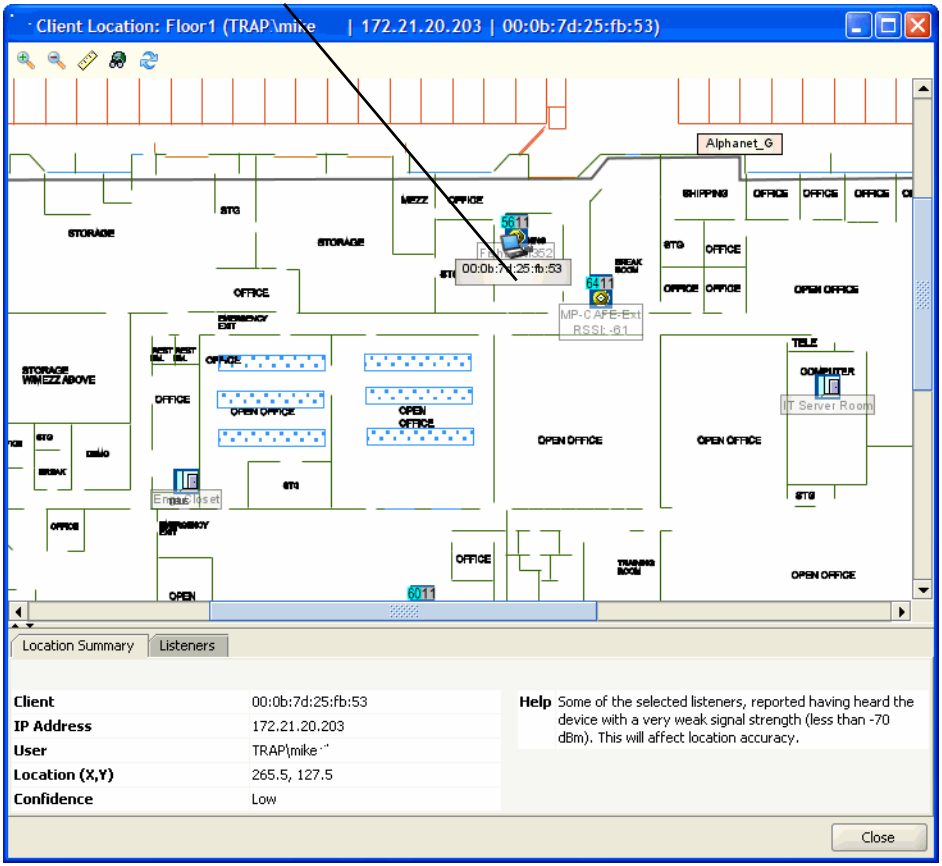
Locate the User

Display the user's approximate location by performing the following steps:

1. On the Find Client(s) Result screen, click the Locate Client task (under Manage). WLAN Management Software retrieves information about the client's location.
2. If three or more APs have not detected the client within 15 seconds of each other, the Listeners Selection dialog box appears, displaying a list of the APs that have detected the client.

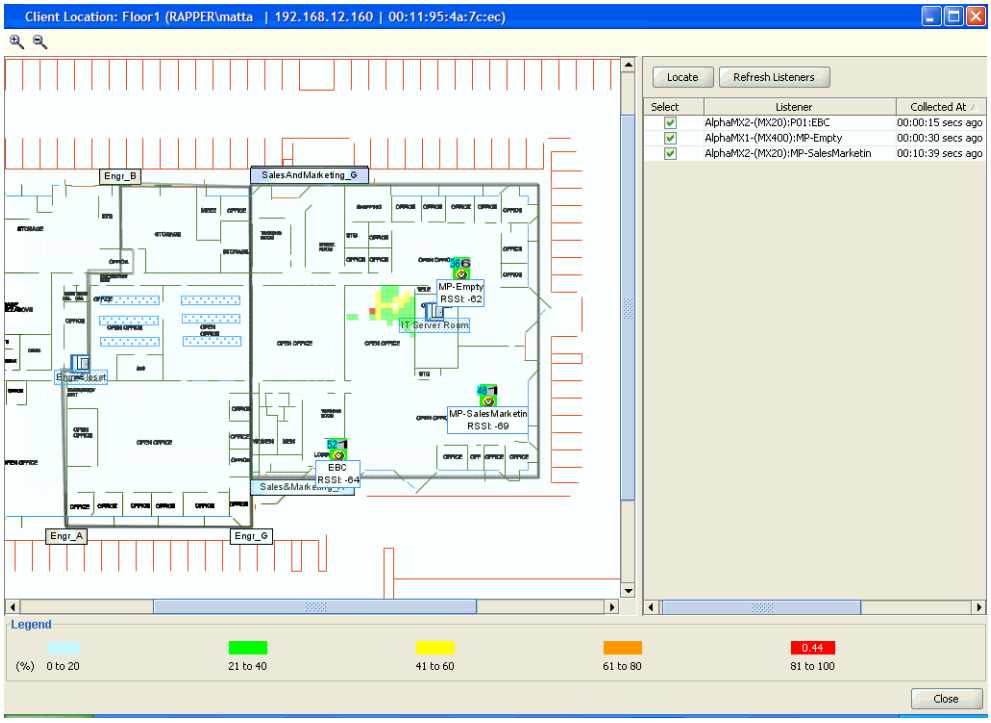
   You can select up to six APs from the list. WMS uses the selected APs to calculate the location of the client.
3. WLAN Management Software displays the approximate location of the client on the floor plan. The client's location is indicated with a laptop icon, as shown below.

Client's Approximate Location



4 To refresh the list of APs that detect the client, click the (Refresh Listeners) button

5 To change the APs used for calculating the client's location, click the Listeners tab and Select or deselect APs from the list, then click the (Locate) button.Click on the Monitor option in the main WLAN Management Software tool bar.

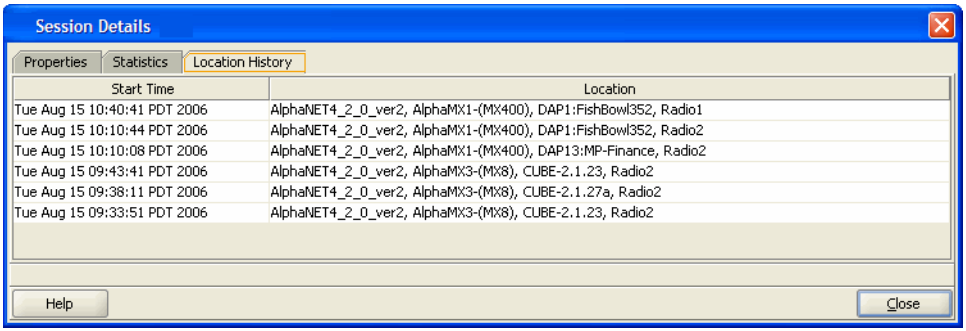


Display User Activity

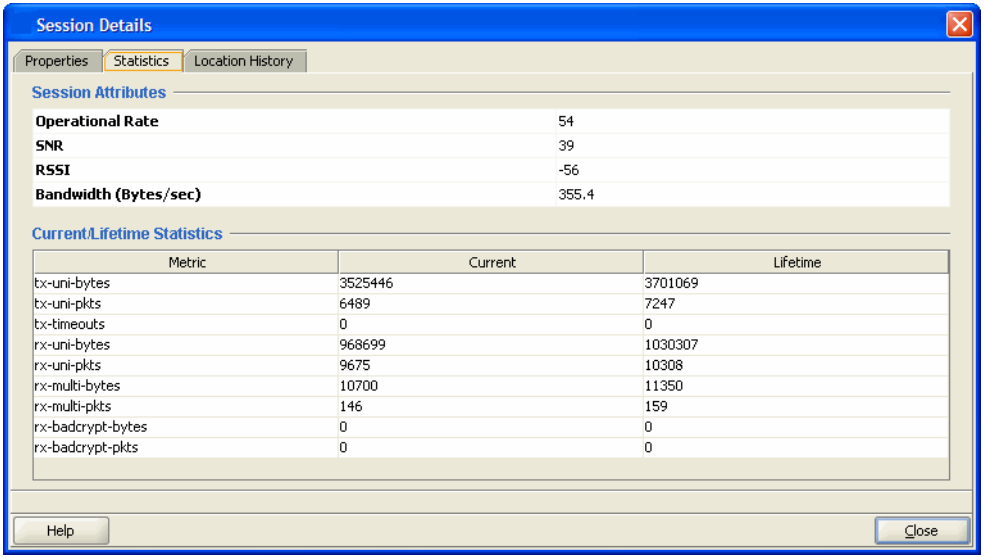
You can display the event types recorded for the user. Disassociation events can occur, and users can be dropped from the network. These events can indicate the reason why access is barred or performance is slow for the user. For example, typical authorization failures occur if the local database or RADIUS server fails to recognize a user.

To display user activity

1. On the Find Client(s) screen, click the Session Details task (under View). WLAN Management Software retrieves information about the client's session.
2. Select the **Location History** tab to see where the user has been. From here, you can determine the areas in the WLAN where interference is occurring.



3 Select the **Statistics** tab to display current and lifetime statistics for the user.

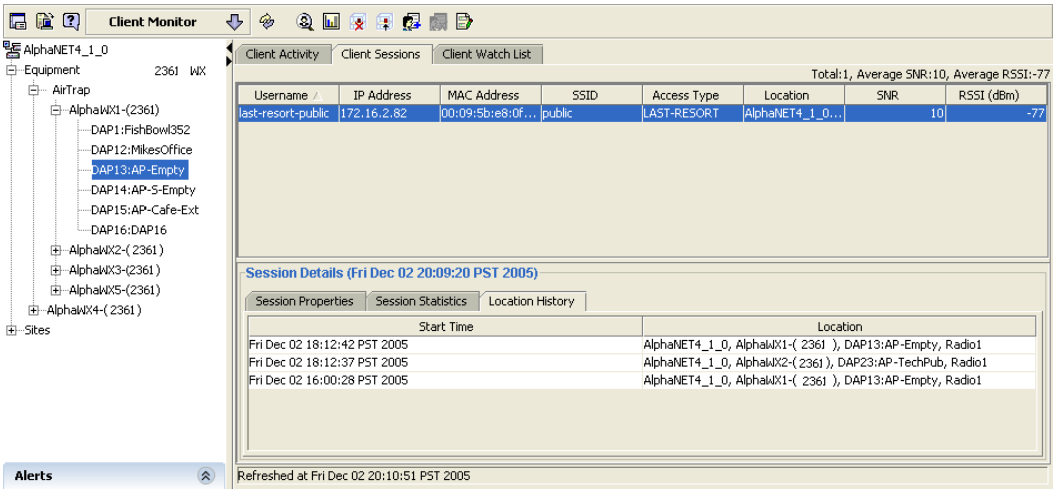


Operational rate statistics display the throughput per second. The following throughput rates are optimum:

- **802.11b–11 Mb/s (optimum)**
- **802.11g/a–36 Mb/s or higher**

Signal to Noise Ratio (SNR) statistics can help you determine whether the interference is being created by too much noise on a channel. Receive Signal Strength (RSSI) statistics can indicate whether a low signal strength is creating the user's performance problem.

A high number of Transmit Timeouts (tx-timeouts) can indicate interference problems.

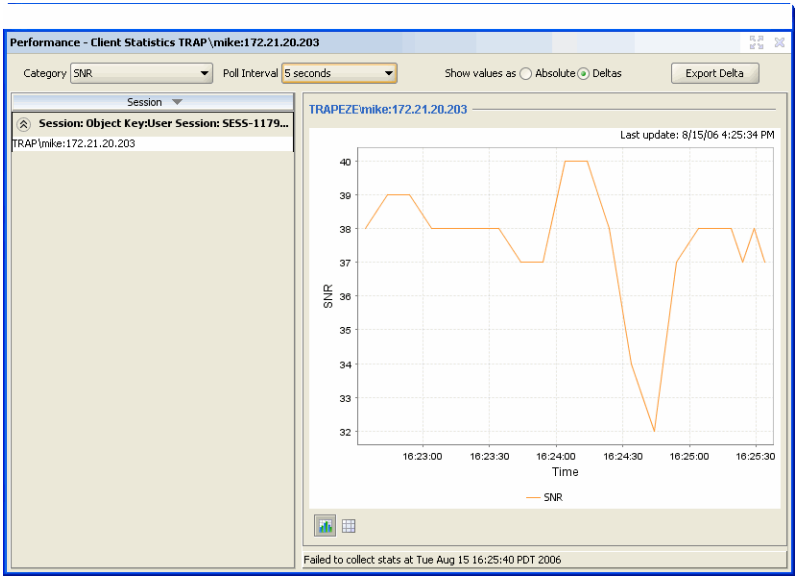


View User Performance Statistics

If the user's complaint cannot be traced to a specific problem based on current activity, you can view statistics over a period of time.

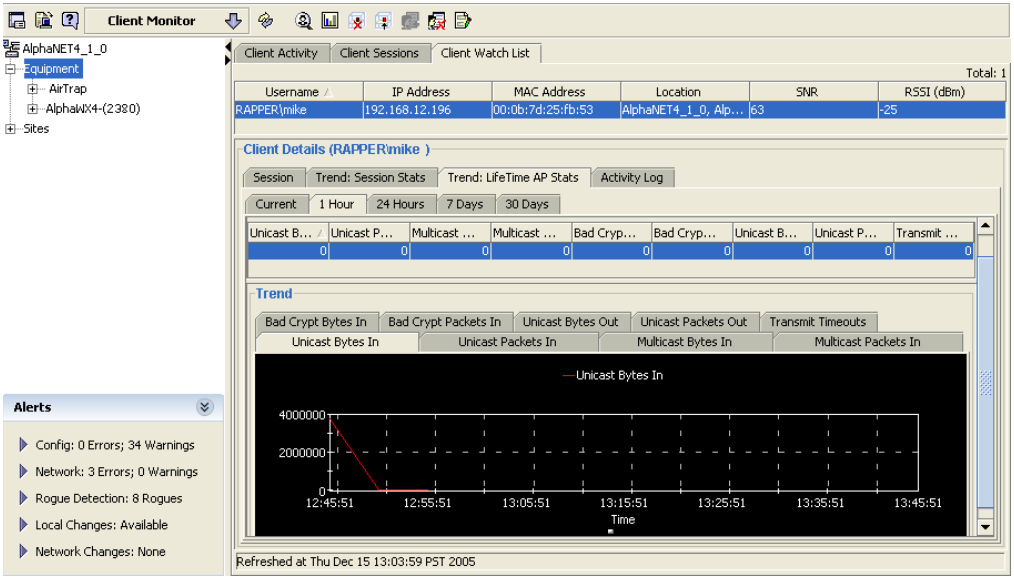
To view user performance statistics

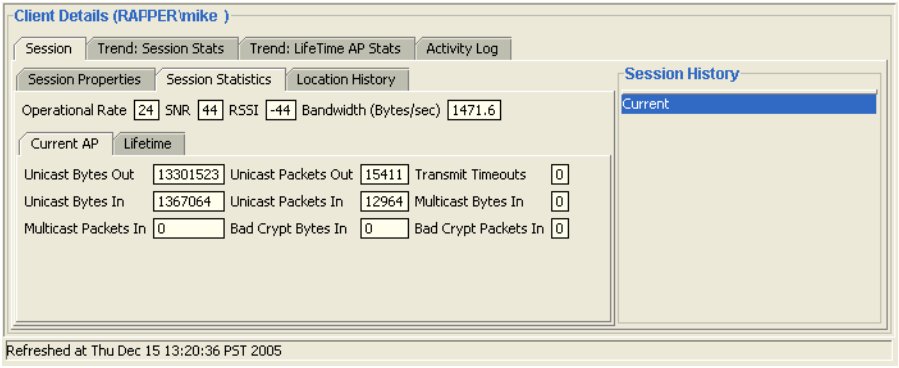
1. Click on the Monitor option in the main WMS tool bar.
2. Click **Details** in the Client Summary View to switch to the Client Monitor View.
3. In the table of Client Sessions in the Content Panel, select the user's session, then click Client Statistics in the Task Panel to display the Performance - Client Statistics dialog for the user.



4 From the Category list, you can select a statistic for which to display information.

5 From the Poll Interval list, you can select how often WLAN Management Software collects the specified statistic for the user.



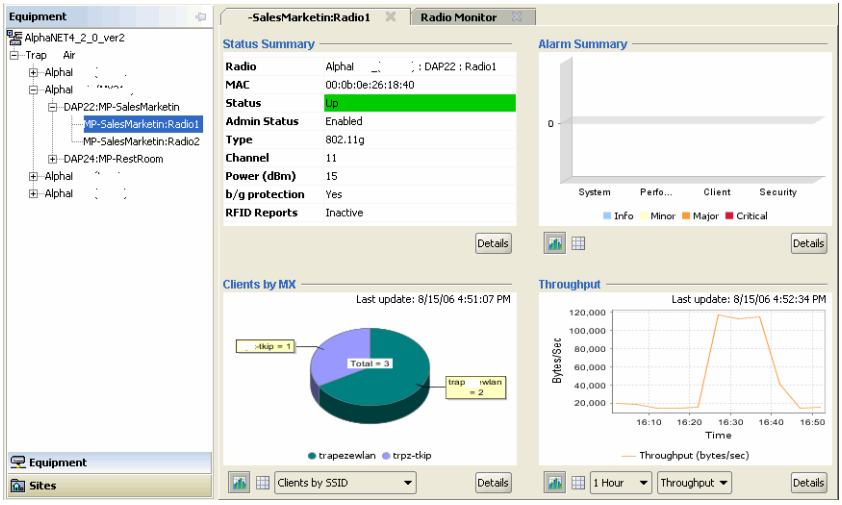

Client Details (RAPPER\mike)
Session
Trend: Session Stats
Trend: LifeTime AP Stats
Activity Log
Session Properties
Session Statistics
Location History
Session History
Current
Operational Rate 24 SNR 44 RSSI -44 Bandwidth (Bytes/sec) 1471.6
Current AP
Lifetime
Unicast Bytes Out 13301523 Unicast Packets Out 15411 Transmit Timeouts 0
Unicast Bytes In 1367064 Unicast Packets In 12964 Multicast Bytes In 0
Multicast Packets In 0 Bad Crypt Bytes In 0 Bad Crypt Packets In 0
Refreshed at Thu Dec 15 13:20:36 PST 2005

Monitor a Group of Users

If a group of users in a specific area of a floor notify you that they are experiencing poor performance, target the radio or radios that the group of users are associating with, and view performance statistics and trends for just those radios.

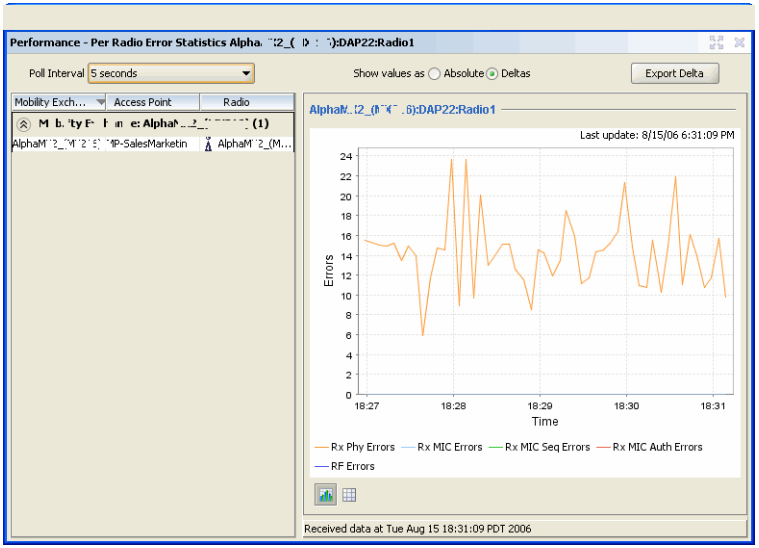
To view performance statistics for an individual radio

1. Click on the Monitor option in the main WLAN Management Software tool bar.
2. Expand the Equipment list in the Organizer panel, and select a radio. Monitor views display summary information for the selected radio.



3. Click **Details** in the Traffic Summary View to switch to the Radio Monitor View.

4 Click on one of the options under Statistics in the Task Panel to display the Performance - Per Radio Statistics dialog for the radio. In the example below, error statistics are displayed.



To view RF trends for an individual radio

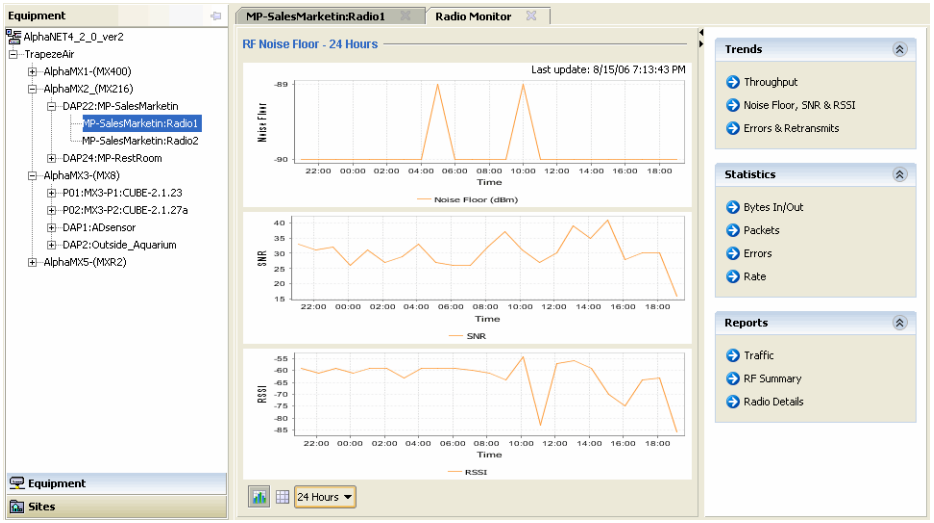
1 Click on the Monitor option in the main WLAN Management Software tool bar.

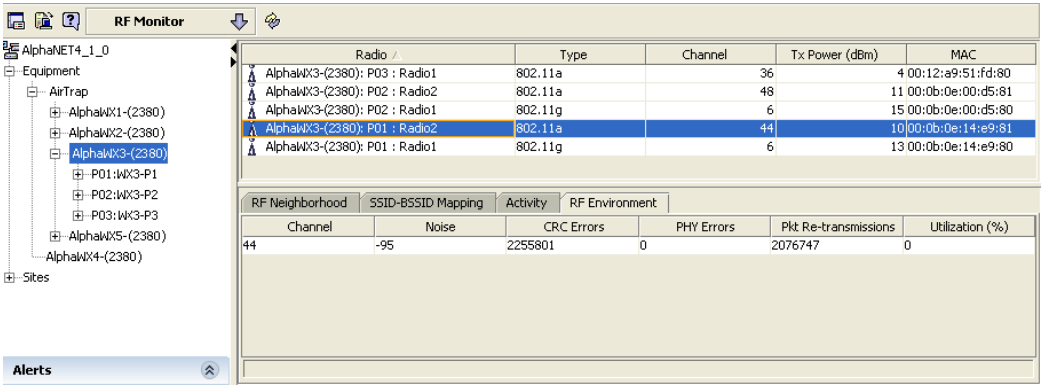
2 Expand the Equipment list in the Organizer panel, and select a radio to display the Monitor views for the radio.

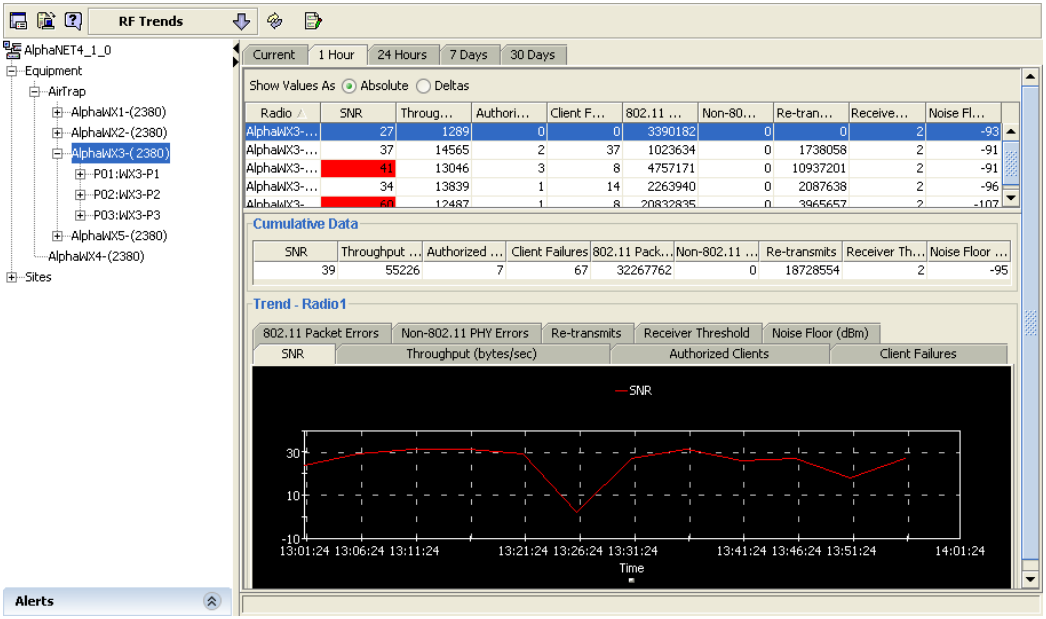
3 Click **Details** in the Traffic Summary View to switch to the Radio Monitor View.

4 Click on one of the options under Trends in the Task Panel to display trend information for the radio. The selected trend information is displayed in the Content Panel.

In the example below, trends for Noise Floor, SNR, and RSSI over the past 24 hours are displayed.


Equipment
AlphaNET4_2_0_ver2
TrapezeAir
AlphaMX1-(MX400)
AlphaMX2_(MX216)
DAP22:MP-SalesMarketin
MP-SalesMarketin:Radio1
MP-SalesMarketin:Radio2
DAP24:MP-RestRoom
AlphaMX3-(MX8)
P01:MX3-P1:CUBE-2.1.23
P02:MX3-P2:CUBE-2.1.27a
DAP1:ADsensor
DAP2:Outside_Aquarium
AlphaMX5-(MXR2)
Equipment
Sites
MP-SalesMarketin:Radio1
Radio Monitor
RF Noise Floor - 24 Hours
Last update: 8/15/06 7:13:43 PM
Noise Floor
Time
Noise Floor (dBm)
SNR
RSSI
24 Hours
Trends
Throughput
Noise Floor, SNR & RSSI
Errors & Retransmits
Statistics
Bytes In/Out
Packets
Errors
Rate
Reports
Traffic
RF Summary
Radio Details


RF Monitor
AlphaNET4_1_0
Equipment
AirTrap
AlphaWX1-(2380)
AlphaWX2-(2380)
AlphaWX3-(2380)
P01:WX3-P1
P02:WX3-P2
P03:WX3-P3
AlphaWX5-(2380)
AlphaWX4-(2380)
Sites
Alerts
Radio
Type
Channel
Tx Power (dBm)
MAC
AlphaWX3-(2380): P03 : Radio1 802.11a 36 4 00:12:a9:51:fd:80
AlphaWX3-(2380): P02 : Radio2 802.11a 48 11 00:0b:0e:00:d5:81
AlphaWX3-(2380): P02 : Radio1 802.11g 6 15 00:0b:0e:00:d5:80
AlphaWX3-(2380): P01 : Radio2 802.11a 44 10 00:0b:0e:14:e9:81
AlphaWX3-(2380): P01 : Radio1 802.11g 6 13 00:0b:0e:14:e9:80
RF Neighborhood
SSID-BSSID Mapping
Activity
RF Environment
Channel
Noise
CRC Errors
PHY Errors
Pkt Re-transmissions
Utilization (%)
44 -95 2255801 0 2076747 0



What's Next?

You can optimize your network by importing RF measurement data to correct RF attenuation obstacle information if you have a reported coverage area problem or if you want to verify your RF network coverage.

- For more information about optimizing your network plan, refer to "Optimizing a Network Plan" on page 201.

Managing Alarms

Set Up the Fault Management System 183
Classify and Organize Faults 185
Manage Faults 186
Store Faults and Retrieve Fault History 189
Generate Alarm Reports 190
Use the Fault Management System to Locate a Rogue 192
What's Next? 200

What Is Fault Management?

The Fault Management System is a feature included in WMS to make it easier to manage faults (alarms) that occur in the network. A fault or alarm (these two terms are used interchangeably) is generated by a trap, a rule, a status, or a threshold-exceeded event. The Fault Management System monitors traps from Nortel and OEM devices.

The Fault Management System also monitors certain traps for third-party applications, and offers administrators the ability to add new trap support when necessary. The type of trap and IP source determine how new trap support should correlate with existing trap support.

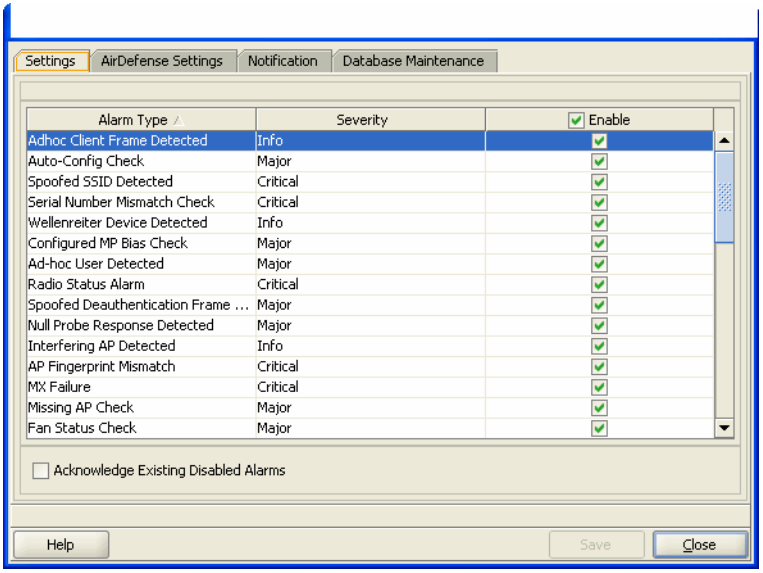
Set Up the Fault Management System

Various types of users have different roles in setting up the Fault Management system. These include users, service administrators, provisioning users, and monitoring users. Serving one of these roles, you may perform the following tasks:

- Customize faults; for example assign severity to faults and set up e-mail notifications.
- Enable or disable faults based on their category or severity.
- Modify fault settings in the Fault Management System, service administrators only.
- Manage the faults and invoke resolutions, if available, provisioning users.
- View faults and acknowledge or unacknowledge the faults, monitoring users.

To set up the Fault Management System

1. Select the **Alarms** option in the main WMS tool bar.
2. Click Setup in the Task Panel. The Alarm Setup dialog is displayed.



3 Select the type of alarms you want to enable by clicking the appropriate check box. Notice that there are several types available for various severity levels.

4 Click the **Notification** tab and select the severity levels for which WMS should send an email notification. You can select severity levels for the following categories:

- **Performance**
- **Security**
- **Client**
- **System**

Enter the appropriate email address in the Email Address field at the bottom of the screen.

5 Click the **Database Maintenance** tab. The Database Maintenance tab allows you to specify how many faults to store in the database and the number of days to keep uncleared faults. In addition, use this tab to specify the number of days to keep active Critical, Major, Minor, and Informational alarms in the database. Enter the desired values in the following fields:

- **Number of events per alarm—The number of recent events that should be retained in the database for each alarm.**
- **Number of days—The number of days after which any cleared alarms will be deleted from the database.**
- **Critical—The number of days after which any active critical alarms will be aged.**
- **Major—The number of days after which any active major will be aged.**
- **Minor—The number of days after which any active minor will be aged.**
- **Informational—The number of days after which any active informational will be aged.**

6 Click **Save** to save your changes, then **Close** to close the dialog.

Classify and Organize Faults

When a fault occurs in WMS, the Fault Management System offers a means to categorize the fault by functional area and severity.

Depending on the functional area in which a fault occurs, the fault can be assigned to one of the following categories:

- System
- Performance
- Security
- Client

WMS also organizes faults by the following severities:

- Critical (Red)
- Major (Orange)
- Minor (Yellow)
- Informational (Blue)

WMS displays a single fault management table that allows you to view all fault-related information, including the fault's functional area and severity, a description of the fault, the WSS that is the source of the fault, the current state of the fault, and tasks you can perform to respond to the fault, including alarm management, resolutions, and reports.

Search Capabilities

WMS users can sort system faults based on any of the columns in the table. WMS sorts fault events on the date of occurrence as Today, Yesterday, Last Week, or Last Month. WMS can also sort faults based on Category, Source, Severity, and Time. Other standard, commonly used filters are also available, such as Current Hour, Current Day, and text search. To perform a text search, type the desired description in the text box located in the alarm filter tool bar.

Use the fault dashboard, shown below, located above the alarm details panel to gather specific data about particular alarms. The lists allow you to filter your results by selecting criteria

Menu items include the following options:

- All Severities
    - **Critical**
    - **Major**
    - **Minor**
    - **Info**
- All Categories
    - **System**
    - **Performance Client**
    - **Security**

- Network Plan
    - **Mobility Domain**
    - **WLAN—Security Switch**
    - **10/100 Ethernet Port**
    - **Gigabit Ethernet Port**
    - **Distributed AP**
    - **AP**
    - **Radio**
    - **Site**
    - **Building**
    - **Floor**
    - **AirDefense Server**
- Network plan name(s)

These options allow you to see a variety of specific alarms for each device in the network.

Manage Faults

By performing various tasks, such as acknowledging, unacknowledging, and deleting faults; you can manage all of the various alarms in WMS. For some faults, WMS provides a list of related tasks that guides you through appropriate tasks and resolutions. Furthermore, when the same operation can manage more than one fault, you can select those multiple faults, and then perform the same appropriate fault management operation simultaneously.

If you have cleared or acknowledged a fault and a new event occurs that correlates to the original cleared or acknowledged fault, reactivate the original fault.

If the WMS server is down for a period of time (an hour or more), all faults in the system will automatically clear once the server restarts. Clearing the faults after down time ensures that all faults in the system are valid.

The Alarms function displays information retrieved from the WLAN Management Software service. WMS presents the data under the WMS tool bar option in the following views:

- Alarm Summary
- Top 5 Sources of Alarms
- IDS Alarms
- DoS Alarms

Alarm Summary

The WMS Fault Management System displays alarm data in three ways: in bar graphs, pie charts, or tables. The default view is the graphical representation of alarms. However, you may switch between the chart and table views by clicking the tabular icon or the graph icon.

Alarm Summary Details

The WMS displays Fault Management data in the Content panel when you click on the Alarms tool bar option. To access the Fault Management System, WMS client must have a connection with the host running the WMS service.

To access Fault Management data

1. Select the **Alarms** option in the main WMS tool bar.
2. To view a table of all alarms in WMS, click **Details** at the bottom right of the Alarm Summary screen. Performing this action produces the same effect as clicking the tabular icon . From the Alarm Summary screen, you can also choose to view a summary of alarm information in other formats.

   You can click the tabular (Show Table) icon or the graph (Show Chart) icon to switch between the chart and table views.

To view Alarm Summary information in table format

1. To view a summary of alarm information in table format, click the tabular icon. By default, the table displays statistics of faults by functional area on the X axis and by severity on the Y axis.

   In the table view, hypertext numbers link to filtered lists that contain only the alarms for that row and column.
2. To view only category data, click *Alarms by Category* in the list at the bottom of the screen.
3. To view only severity data, click *Alarms by Severity* in the list at the bottom of the screen.

To view Alarm Summary information in pie chart format

You can view alarm summary information via pie charts in two different formats: by category and by severity.

1. To view a summary of alarm information by category, from the list at the bottom left of the Alarm Summary screen, select the show chart icon, and then click *Alarms by Category.*
2. To view a summary of alarm information by severity, select *Alarms by Category* from the list at the bottom left of the Alarm Summary screen, and then click the show chart icon. WMS displays a pie chart with a summary of alarms by severity, as shown in the following screen.

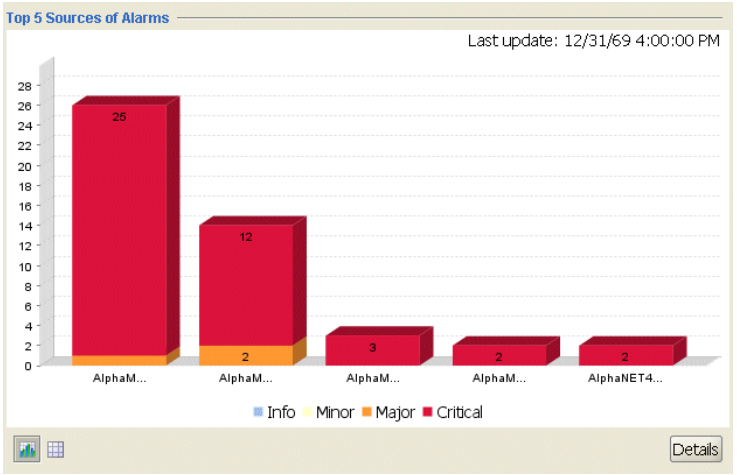
Top 5 Sources of Alarms

Sources are the separate WSSs in the network plan.

To view the top 5 sources of alarms in chart format

1. Click the chart icon at the bottom left corner of the Top 5 Sources of Alarms section of the WMS screen.

Each bar in the graph shows the alarms that are generated by a specific WSS in the network plan, depicted in the following screen



2 To view a table of all alarms in WMS, click the **Details** button in the Top 5 Sources of Alarms section. Performing this action produces the same effect as clicking the show table icon.

Intrusion Detection System (IDS) Alarms

WLAN Management Software generates alarms when network intrusion events are detected, such as when rogue APs appear on the network, and when clients associate with the rogue APs. SNMP notifications must be enabled on the WSSs in order for alarms to appear in WLAN Management Software.

To view IDS alarms

1 To view IDS alarms in chart format, click the chart icon at the bottom left corner of the IDS Alarms section of the WMS screen.

2 To view IDS alarms in table format, click the table icon at the bottom left corner of the IDS Alarms section of the WMS screen.

3 To view a table of all alarms in WMS, click **Details** at the bottom of the IDS Alarms section of the WMS screen. Performing this action produces the same effect as clicking the show table icon.

Denial of Service (DoS) Alarms

WLAN Management Software generates alarms when attempts at Denial of Service attacks are detected on the network. SNMP notifications must be enabled on the WSSs in order for alarms to appear in WLAN Management Software.

To view DoS alarms

1 To view DoS alarms in chart format, click the chart icon at the bottom left corner of the DoS Alarms section of the WMS screen.

2 To view alarms in table format, click the table icon at the bottom left corner of the DoS Alarms section of the WMS screen.

In the table view that displays, hypertext numbers link to filtered lists that contain only the alarms for that row and column that contain the hypertext.

3 To view a table of all alarms in WMS, click **Details** at the bottom of the DoS Alarms section of the WMS screen. Performing this action produces the same effect as clicking the show table icon.

Store Faults and Retrieve Fault History

WMS stores fault information on the server database and allows multiple clients to access the data. With each fault stored in the database, correlated traps and events are also stored. Data is periodically purged to keep the database to a manageable size. Purging is based on criteria such as the number of active faults (events) or the number of days for which data should be preserved.

In addition to active fault information, the database also holds historic fault information. You can view this historic information when necessary. However, the information is available for viewing in reports only. Consequently, you cannot perform any action on historic information.

To retrieve fault history

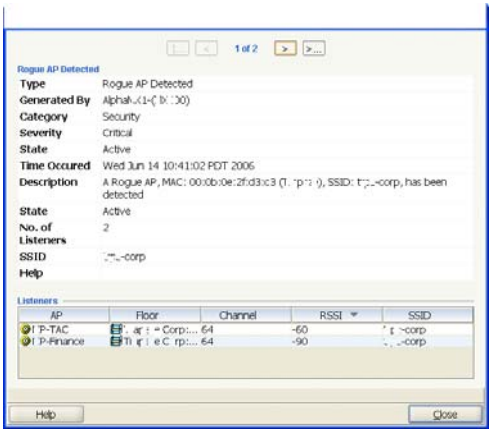
1 Click **History** in the Task panel under Alarms.

2 WMS displays the Alarm History dialog box. You can sort the history results by any of the following column headings:

- **Date**
- **Severity**
- **Category**
- **Description**
- **Object**
- **State**

3 Click on a row to view the details of a specific alarm in the tabular view.

4 After clicking on a row, WMS will display more information for the specific alarm in the lower pane. Click a row in the lower pane to view all of the details for the alarm, or click **Event Details** in the Alarms panel on the right. WMS will display a window similar to the one shown in the following screen.



5 Click Close in the lower right corner.

Generate Alarm Reports

WMS provides the capability to export fault data in the form of reports. You can generate the following reports:

- Alarm Summary—Provides the total number of current faults in the system and identifies them by type, source, severity or state.
- Alarm History—Provides a list of all faults in the system that were active within a specified time period. Users can sort the faults by source, severity, or category.
- Security—Provides a report of DoS and IDS alarms.
- Client OUI—Provides a list of alarms according to the Organizationally Unique Identifier of the client for which the alarms were generated.

Alarm Summary Report

The Alarm Summary report provides an overall view of total current faults in the system. The report identifies the faults by type, source, severity, or state.

To generate an Alarm Summary report

1 Click **Alarm Summary** in the Task panel under Reports. The Alarm Summary Report dialog box appears.

2 Select one of the following Report Scope Types:

- **Network Plan**
- **Mobility Domain**
- **Site**
- **Building**

- **Floor**

3. Select the desired Report Scope Instance in the list.
4. If necessary, browse to the desired output directory by clicking in the Output Directory box. Navigate to the desired location and click **Select**.
5. Click **Generate** in the bottom right corner.
6. After the report generation is complete, click the blue hyperlink in the Results box to view the report. The report will open in a new window and will be saved at the previously selected location.
7. Click **Close** in the bottom right corner of the Alarm Summary Report dialog box.

Alarm History Report

The Fault History report provides a list of all faults in the system that were active within a specified time period. WMS allows you to sort the faults by source, severity, or category.

To generate an Alarm History report

1. Click **Alarm History** in the Task panel under Reports. The Alarm History Report dialog box appears.
2. Select the desired Report Scope type from the list. You can select one of the following scope types:
   - **Network Plan**
   - **Mobility Domain**
   - **Site**
   - **Building**
   - **Floor**
3. Select the desired Report Scope instance from the list.
4. Enter the date you would like the report to begin in the *Start Date* field or navigate to the desired date from the calendar.
5. Enter the desired *Start Time* in the field or navigate through the up or down arrows.
6. Enter the date you would like the report to end in the *End Date* field or navigate to the desired date from the calendar.
7. Enter the desired *End Time* in the field or navigate through the up or down arrows.
8. If necessary, browse to the desired output directory in the Output Directory box. Navigate to the desired location and click **Select**.
9. Click **Generate** in the bottom right corner.
10. After generating the report, click the blue hyperlink in the Results box to view the report. WMS opens the report in a new window and saves it at the previously selected location.
11. Click **Close** in the bottom right corner of the Alarm Summary Report dialog box.

- Security—Provides a report of DoS and IDS alarms.
- Client OUI—Provides a list of alarms according to the Organizationally Unique Identifier of the client for which the alarms were generated.

Security and Client OUI Reports

Security reports list DoS and IDS alarms, and Client OUI reports list alarms according to the Organizationally Unique Identifier of the client for which the alarms were generated. The procedure for generating both types of reports is the same.

To generate a Security or Client OUI report

1. Select the **Reports** option in the main WMS tool bar.
2. Select Alarm Reports in the Report Category column.
3. Select the Report type from the Reports list.
4. If necessary, browse to the desired output directory in the Output Directory box. Navigate to the desired location and click **Select**.
5. Click **Generate** in the bottom right corner.
6. After generating the report, click the blue hyperlink in the Results box to view the report. WMS opens the report in a new window and saves it at the previously selected location.
7. Click **Close** in the bottom right corner of the Report dialog box.

Use the Fault Management System to Locate a Rogue

This section provides an example of how you can use the Fault Management system to locate rogue devices on your network, then configure WSS Software to use countermeasures against them.

AP radios automatically scan the RF spectrum for other devices transmitting in the same spectrum. The RF scans discover third-party transmitters in addition to other Nortel radios. WSS Software considers the non-Nortel transmitters to be devices of interest, which are potential rogues.

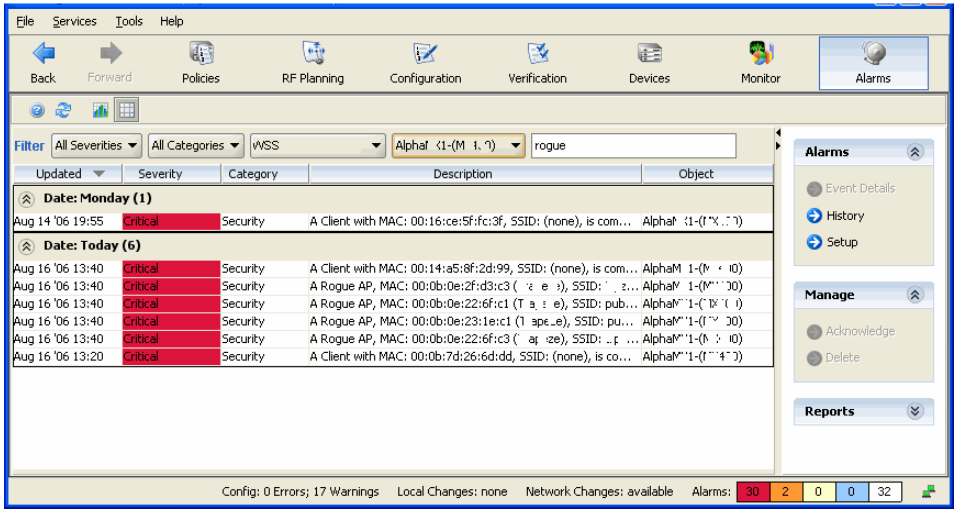
A rogue access point is an access point that is not authorized to operate in your network. Rogue access points and their clients undermine the security of an enterprise network by potentially allowing unchallenged access to the network by any wireless user or client in the physical vicinity. Rogue access points and users can also interfere with the operation of your enterprise network. You can configure WMS to automatically use countermeasures against rogue APs to disable them.

Not all access points placed on the rogue list are “hostile” rogues. You may want to move some of the access points from the rogue list to a known devices list or a third-party AP list. For more information about this topic as well as more detailed information about combatting rogues, see the chapter “Detecting and Combatting Rogue Devices” in the *Nortel WLAN Management Software 2300 Series Reference Guide.*

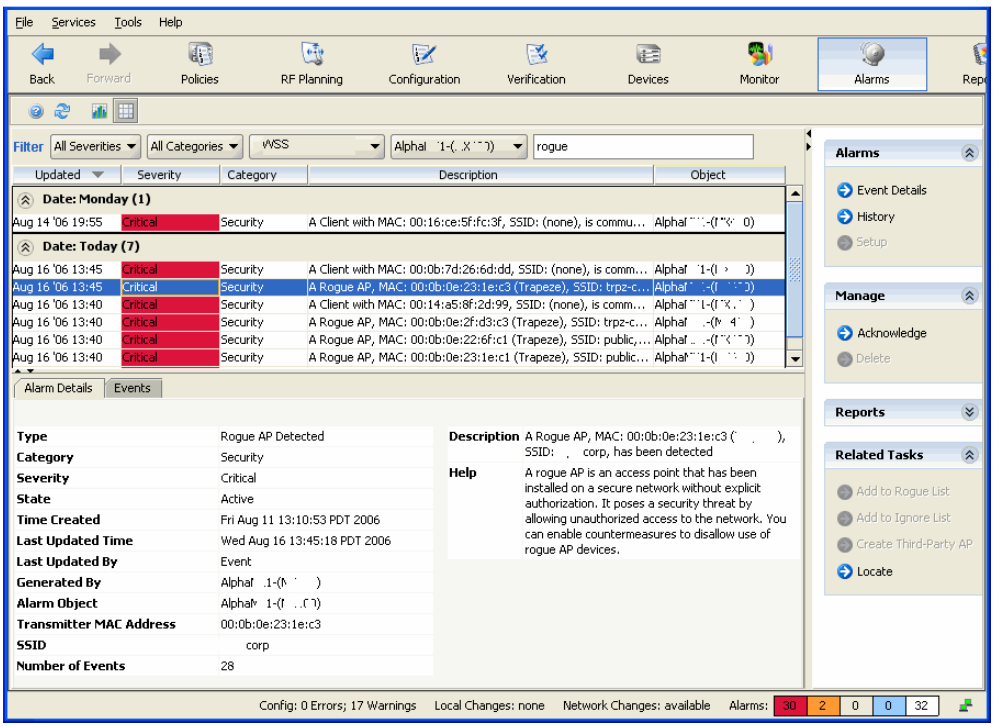
To locate a rogue

1. Click on the Alarms option in the main WLAN Management Software tool bar. A list of alarms is displayed.
2. Filter the alarm list so that only alarms related to rogue devices are displayed.

   To do this, adjust the selection criteria on the fault dashboard. In the example below, the alarms are filtered so that only alarms from the WSS AlphaWSS1-(2380) that contain “rogue” in the Description field are displayed.


File Services Tools Help
Back Forward Policies RF Planning Configuration Verification Devices Monitor Alarms
Filter All Severities All Categories WSS rogue
Updated Severity Category Description Object
Date: Monday (1)
Aug 14 '06 19:55 Critical Security A Client with MAC: 00:16:ce:5f:fc:3f, SSID: (none), is com...
Date: Today (6)
Aug 16 '06 13:40 Critical Security A Client with MAC: 00:14:a5:8f:2d:99, SSID: (none), is com...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:2f:d3:c3 ( ), SSID:
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:22:6f:c1 (T), SSID: pub...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:23:1e:c1 (T), SSID: pu...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:22:6f:c3 ( ), SSID:
Aug 16 '06 13:20 Critical Security A Client with MAC: 00:0b:7d:26:6d:dd, SSID: (none), is co...
Alarms
Event Details
History
Setup
Manage
Acknowledge
Delete
Reports
Config: 0 Errors; 17 Warnings Local Changes: none Network Changes: available Alarms: 30 2 0 0 32

3 Click on one of the alarms to display details about the alarm.

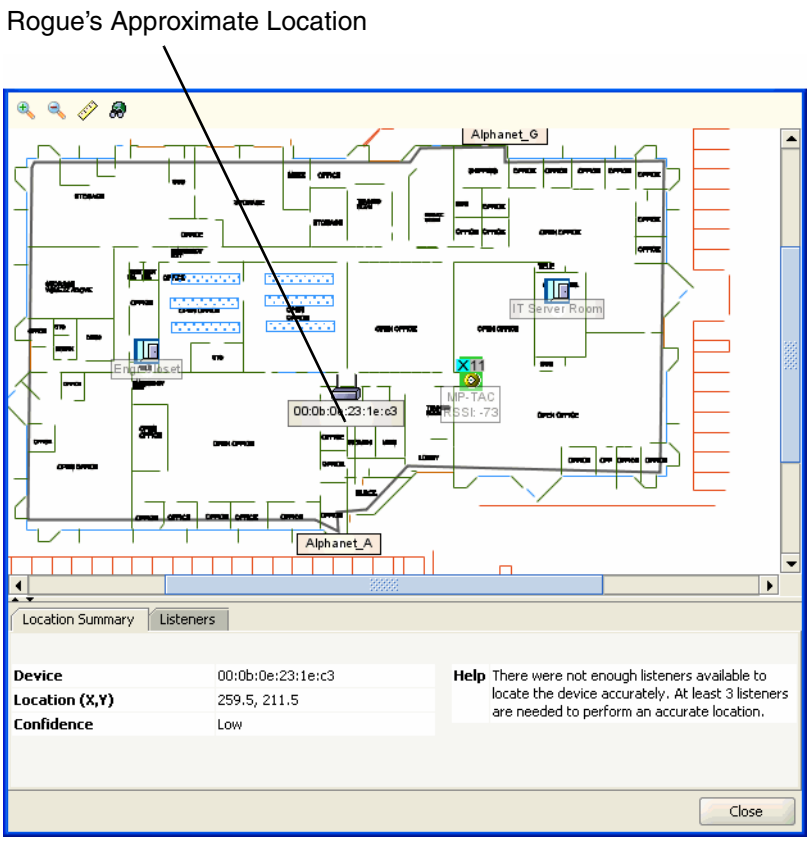

File Services Tools Help
Back Forward Policies RF Planning Configuration Verification Devices Monitor Alarms
Filter All Severities All Categories WSS rogue
Updated Severity Category Description Object
Date: Monday (1)
Aug 14 '06 19:55 Critical Security A Client with MAC: 00:16:ce:5f:fc:3f, SSID: (none), is commu...
Date: Today (7)
Aug 16 '06 13:45 Critical Security A Client with MAC: 00:0b:7d:26:6d:dd, SSID: (none), is comm...
Aug 16 '06 13:45 Critical Security A Rogue AP, MAC: 00:0b:0e:23:1e:c3 (Trapeze), SSID: trpz-c...
Aug 16 '06 13:40 Critical Security A Client with MAC: 00:14:a5:8f:2d:99, SSID: (none), is comm...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:2f:d3:c3 (Trapeze), SSID: trpz-c...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:22:6f:c1 (Trapeze), SSID: public,...
Aug 16 '06 13:40 Critical Security A Rogue AP, MAC: 00:0b:0e:23:1e:c1 (Trapeze), SSID: public...
Alarm Details Events
Type Rogue AP Detected
Category Security
Severity Critical
State Active
Time Created Fri Aug 11 13:10:53 PDT 2006
Last Updated Time Wed Aug 16 13:45:18 PDT 2006
Last Updated By Event
Generated By
Alarm Object
Transmitter MAC Address 00:0b:0e:23:1e:c3
SSID corp
Number of Events 28
Description A Rogue AP, MAC: 00:0b:0e:23:1e:c3 ( ), SSID: , corp, has been detected
Help A rogue AP is an access point that has been installed on a secure network without explicit authorization. It poses a security threat by allowing unauthorized access to the network. You can enable countermeasures to disallow use of rogue AP devices.
Alarms
Event Details
History
Setup
Manage
Acknowledge
Delete
Reports
Related Tasks
Add to Rogue List
Add to Ignore List
Create Third-Party AP
Locate
Config: 0 Errors; 17 Warnings Local Changes: none Network Changes: available Alarms: 30 2 0 0 32

4 Click the Events tab to display events WLAN Management Software has recorded about the rogue.

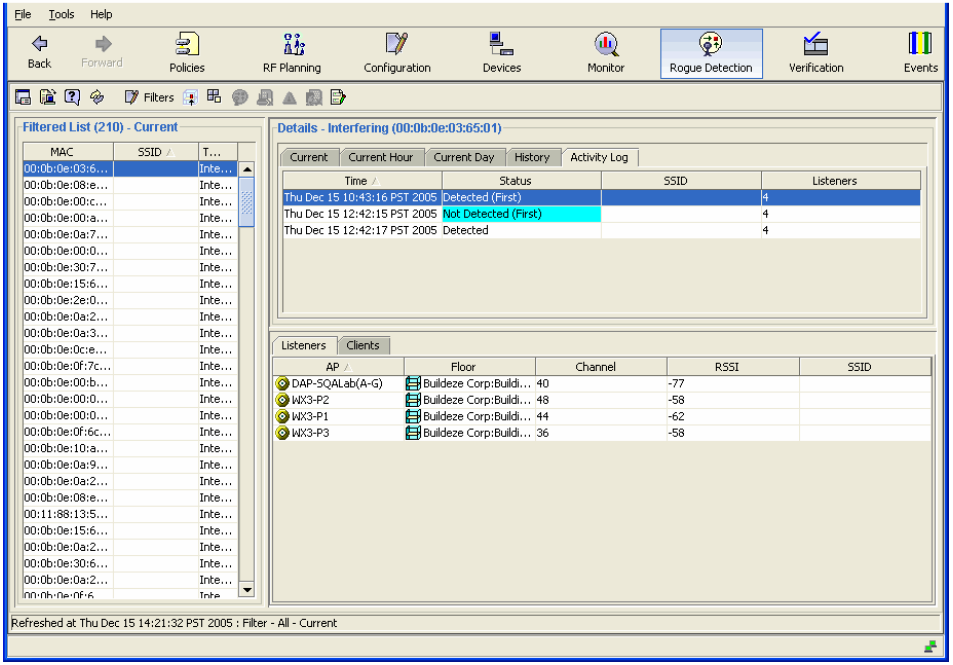
The number of listeners (other APs) that detected the rogue are displayed. The larger the number of listeners detecting the rogue, the easier it is for WMS to locate the rogue in the RF coverage area.

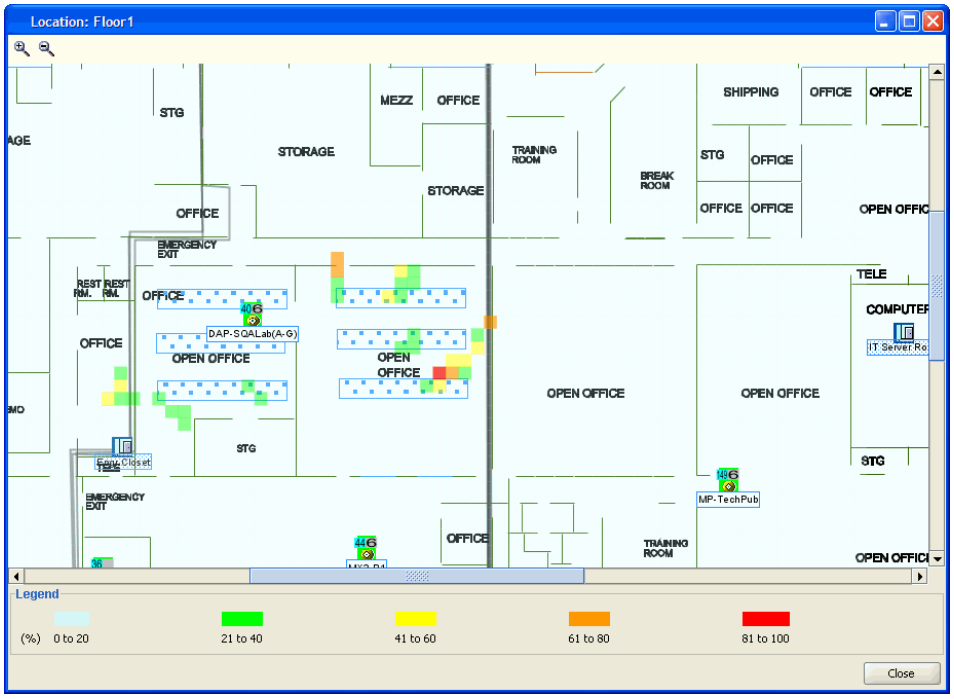
5 Locate the rogue in the RF coverage area. In the Task Panel, under Related Tasks, click Locate.

The approximate location of the rogue is displayed in the RF coverage area.



6 To change the APs used for calculating the rogue's location, click the Listeners tab and select or deselect APs from the list, then click the (Locate) button.


File
Tools
Help
Back
Forward
Policies
RF Planning
Configuration
Devices
Monitor
Rogue Detection
Verification
Events
Filters
Filtered List (210) - Current
MAC
SSID
T...
Details - Interfering (00:0b:0e:03:65:01)
Current
Current Hour
Current Day
History
Activity Log
Time
Status
SSID
Listeners
Thu Dec 15 10:43:16 PST 2005 Detected (First) 4
Thu Dec 15 12:42:15 PST 2005 Not Detected (First) 4
Thu Dec 15 12:42:17 PST 2005 Detected 4
Listeners
Clients
AP
Floor
Channel
RSSI
SSID
DAP-SQALab(A-G) Buildeze Corp:Buildi... 40 -77
WX3-P2 Buildeze Corp:Buildi... 48 -58
WX3-P1 Buildeze Corp:Buildi... 44 -62
WX3-P3 Buildeze Corp:Buildi... 36 -58
Refreshed at Thu Dec 15 14:21:32 PST 2005 : Filter - All - Current



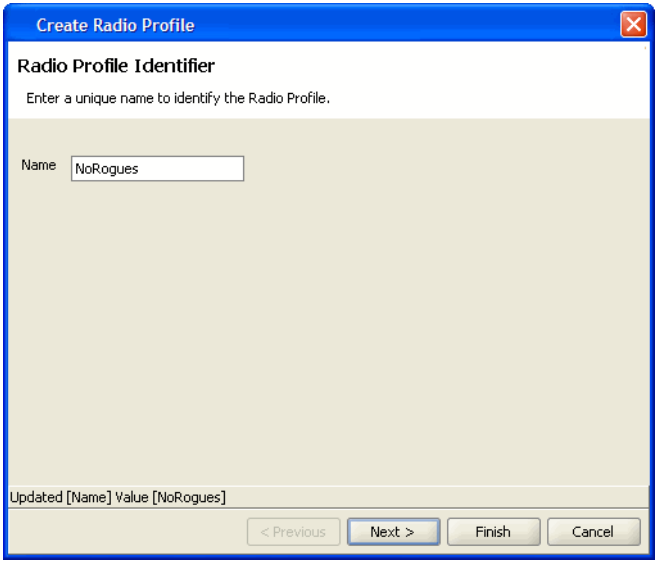
Configuring Countermeasures

You can enable WSS Software to use countermeasures against rogues. Countermeasures consist of packets that interfere with a client's ability to use the rogue. Countermeasures are disabled by default. When you enable them, all devices of interest that are not in the known devices list become viable targets for countermeasures.

Countermeasures are enabled on an individual radio profile basis. When you create a radio profile, you can apply it to specified service profiles or to individual radios. The following example shows how to create a radio profile, apply the radio profile to AP radios, then enable countermeasures in the radio profile.

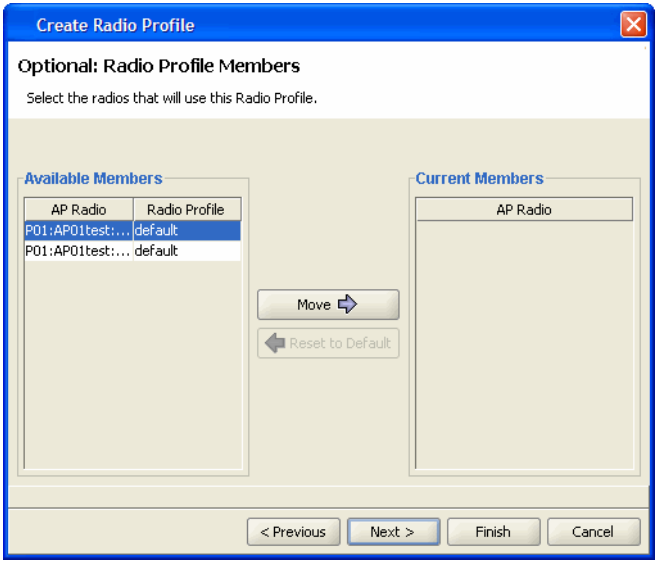
To enable countermeasures

1. Click on the Configuration option in the main WLAN Management Software tool bar.
2. In the Organizer panel, click the plus sign next to the WSS.
3. Click the plus sign next to Wireless.
4. Select Radio Profiles.



5 Click on Create Radio Profile under the Create section of the Task panel. The Create Radio Profile wizard appears.

6 In the Name box, type the name of the radio profile (1 to 16 characters, with no spaces or tabs), and click **Next**. The Radio Profile Members page appears.

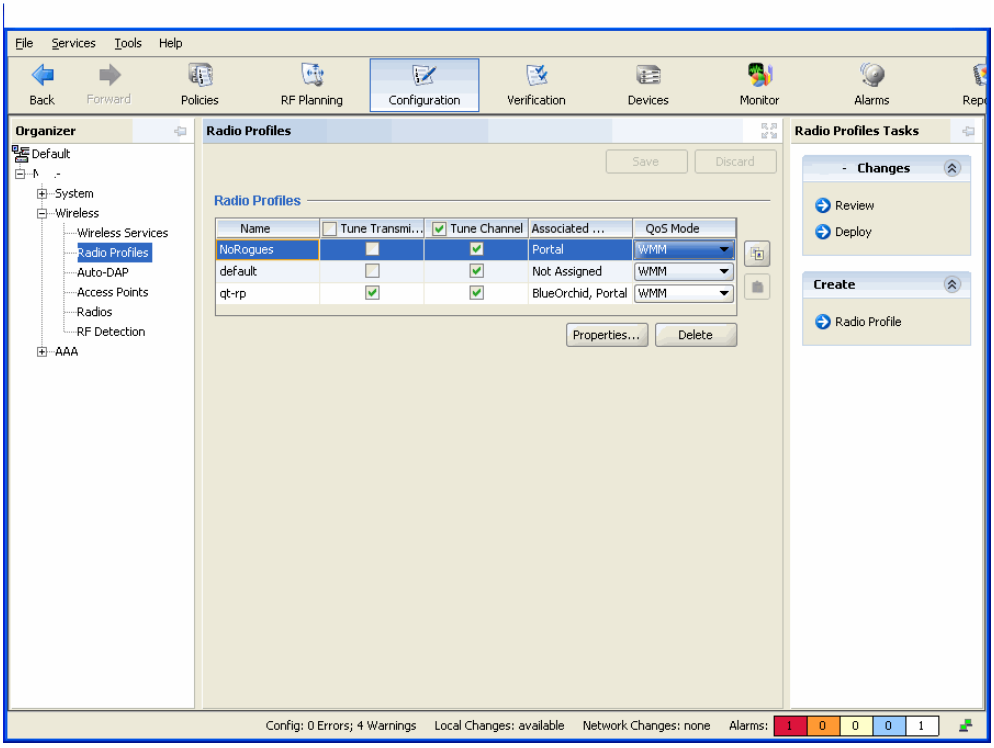


7 Select the AP radios on which you want to enable countermeasures from the Available Members column, and click **Move** to move the radios to the Current Members column.

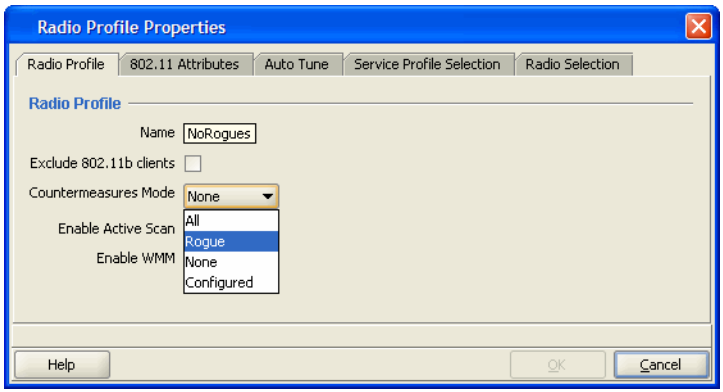
8 Click **Next**. The Radio Profile Service Selection page appears.

9 To map the radio profile to a service profile, select the service profile in the Available Service Profiles list and click **Add**.

10 Click **Finish**. The new radio profile appears in the Radio Profiles table in the Content panel.



11 Select the radio profile you created and click the properties button. The Radio Profile Properties dialog box is displayed.



12 To enable countermeasures against rogues detected by radios managed by this profile, select one of the following from the Countermeasures Mode pull-down list:

- **None—Radios do not use countermeasures. This is the default.**
- **All—Radios use countermeasures against devices classified by WSS Software as rogues and against devices classified by WSS Software as interfering devices.**

  A rogue is a device that is in the Nortel network but does not belong there. An interfering device is not part of the Nortel network but also is not a rogue. WSS Software classifies a device as an interfering device if no client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDB) of any WSS in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with AP radios.

- **Rogue—Radios use countermeasures against devices classified by WSS Software as rogues, but do not use countermeasures against devices classified by WSS Software as interfering devices.**

Caution! Countermeasures affect wireless service on a radio. When an AP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

- **Configured—Causes radios to attack only devices specified in the attack list on the WSS (on-demand countermeasures). When this option is used, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.**

13 To disable active scanning for rogue devices, deselect Enable Active Scan.

When active scan is enabled, radios send *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points. Radios also passively scan by listening for beacons and probe responses. When active scan is disabled, radios perform passive scanning only.

14 Click **Finish** to save the changes and close the wizard.

To verify that countermeasures are being taken against the rogue

1. Click on the Alarms option in the main WLAN Management Software tool bar.
2. Select the rogue in the alarm list. The alarm details panel for the rogue shows countermeasure activity.

   If countermeasures start, stop, and start again, the rogue may have left the area, then returned, or another AP in the coverage area may have taken over countermeasure activities from the last AP to detect the rogue.

What's Next?

After you have managed any existing faults, you can continue to monitor your network.

- For information about monitoring your network, see "Managing and Monitoring Your Network" on page 161.

Optimizing a Network Plan

Using RF Measurements from APs 201
Using RF Measurements from an Ekahau Site Survey 202
Optimizing the RF Coverage Model 208
Locating and Fixing Coverage Holes 209
What's Next? 211

Optimizing your network is a post-deployment technique. To optimize your WLAN, import RF measurement data to correct RF attenuation obstacle information in your network plan. The following are reasons to optimize your network plan:

- You have a reported coverage problem in your network
- You want to verify your network RF coverage

The RF measurement data you use to optimize your network plan can originate from the following:

- APs in your network. You can leverage the RF measurements derived from your APs. If you choose to use RF measurement data from the APs in your network, the data is determined against a smaller set of RF measurements.
- An Ekahau Site Survey™ tool. You perform a site survey of your network. The benefit of using RF measurements derived from a site survey is that the results more closely match the coverage environment that your wireless users experience in your network. Thousands of measurements can be recorded, creating a set of RF measurements that are more precise than those gained from your deployed APs.
- Both APs and a site survey.

By importing data and applying it to your network plan, you correct the RF model to reflect what the measurements report. You update the RF attenuation for obstacles based on real-world measurements. You can then replan your network to achieve the following:

- Make changes in the software to improve signal strength and coverage for groups or individuals
- Modify AP locations
- Add additional equipment to your network

The following sections describe how to import RF measurements from your network, or how to import RF measurements from an Ekahau site survey.

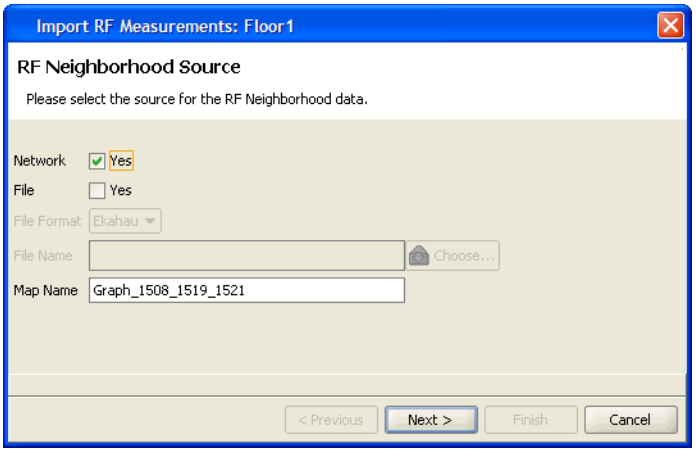
Using RF Measurements from APs

You can apply the RF measurements derived from the APs in your WLAN (which regularly monitors the RF environment) to your network plan. The RF measurements are taken from AP radios.

After you apply the RF measurements, the floor's RF model (obstacles) will be optimized with this data.

To import RF measurements from APs

1. Select the RF Planning option in the main WLAN Management Software tool bar.
2. Display the floor plan in the Content panel.
3. In the Task List panel, click RF Planning.
4. Under Site Survey, click Import Measurement. The Import RF Measurements wizard is displayed.



5. Select **Yes** next to Network.
6. Click **Next**.

   The import progress is displayed. When the import is done, click **Finish** to accept the changes and close the wizard.

After you apply the network RF measurements, you correct the attenuation factors for the floor. Go to "Optimizing the RF Coverage Model" on page 208 for information about this topic.

Using RF Measurements from an Ekahau Site Survey

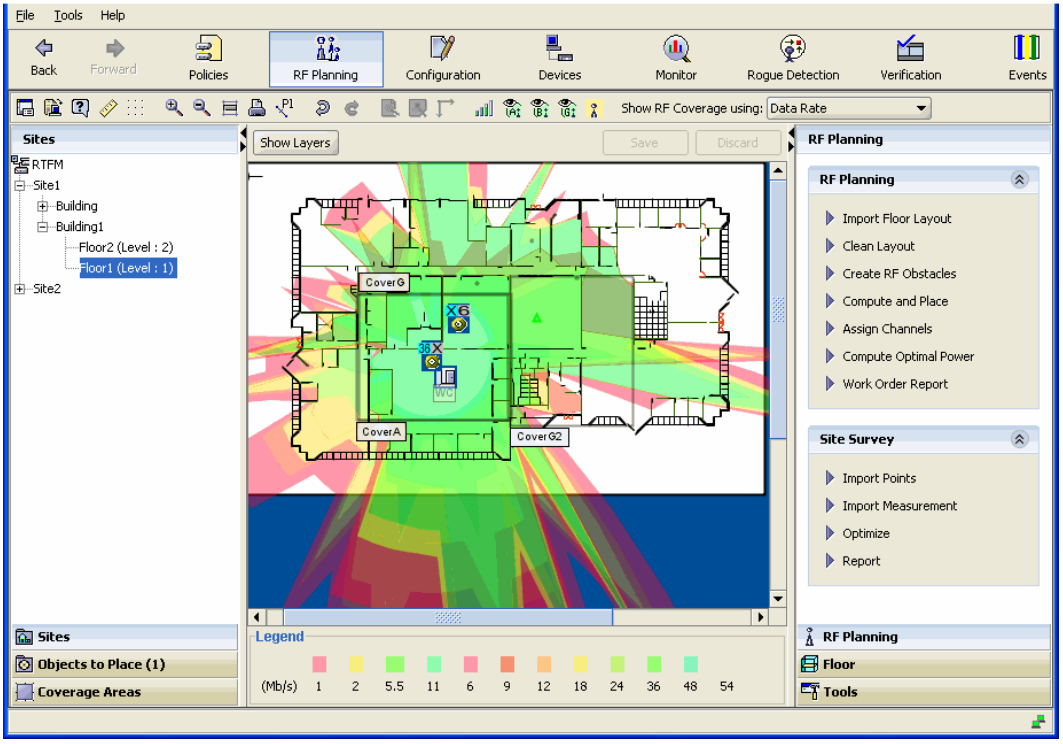
RF measurements come from a site survey file generated by the Ekahau Site Survey tool. Choose one of the following to perform a site survey:

- In WLAN Management Software—View your RF coverage area.
- In WLAN Management Software—Generate a site survey work order, specifying the area you want to survey. A JPEG (.jpeg, .jpg) file is generated.
- Import the generated JPEG file into the Ekahau Site Survey tool.
- Set the scale of the drawing.
- Perform the site survey. Walk through the area, taking measurements with the tool.
- Save the RF measurements in the Ekahau Site Survey tool to a file in comma-separated values (csv) format.
- In WLAN Management Software—Import the csv file containing the RF measurements into WMS.

- In WLAN Management Software—Optimize to correct attenuation factors.

The chapter guides you through the tasks you need to do in WMS. For information about tasks you need to do in the Ekahau Site Survey tool, please refer to the ESS tool's documentation.

The site survey example in this chapter is based on the RF coverage area that follows. For information about displaying RF coverage areas, refer to "Displaying the RF Coverage Area" on page 210.



Generating an Ekahau Site Survey Work Order

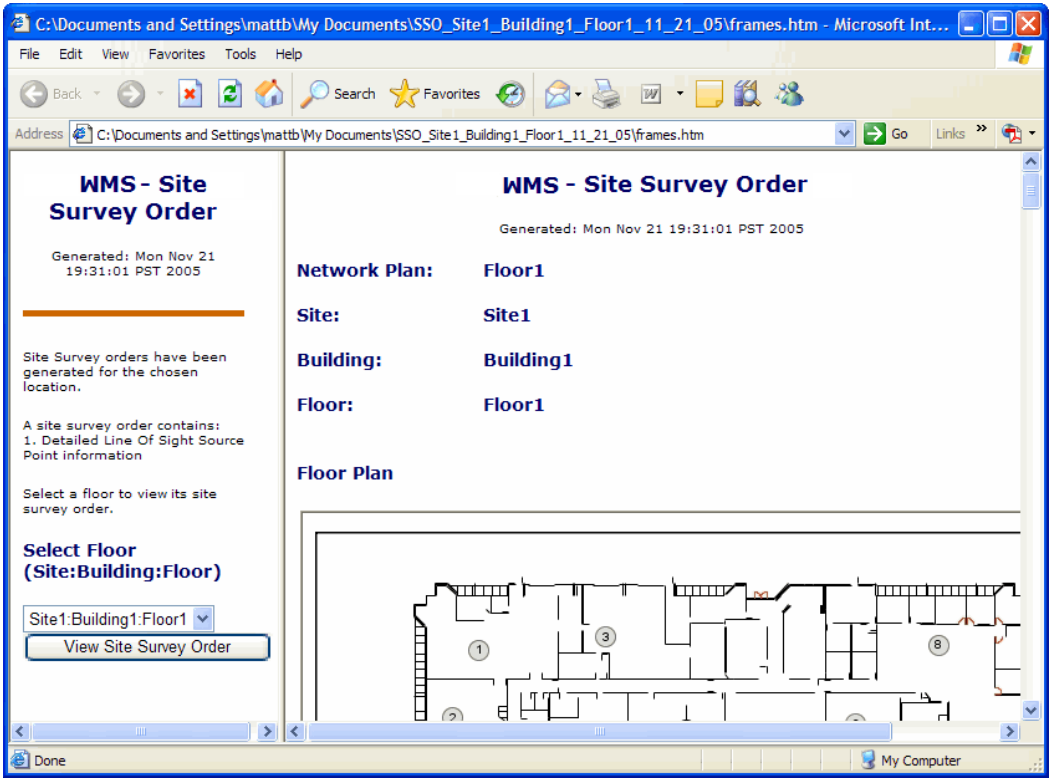
The site survey order contains the locations and MAC addresses of the APs for use when conducting a site survey, and also provides a JPEG image of the floor.

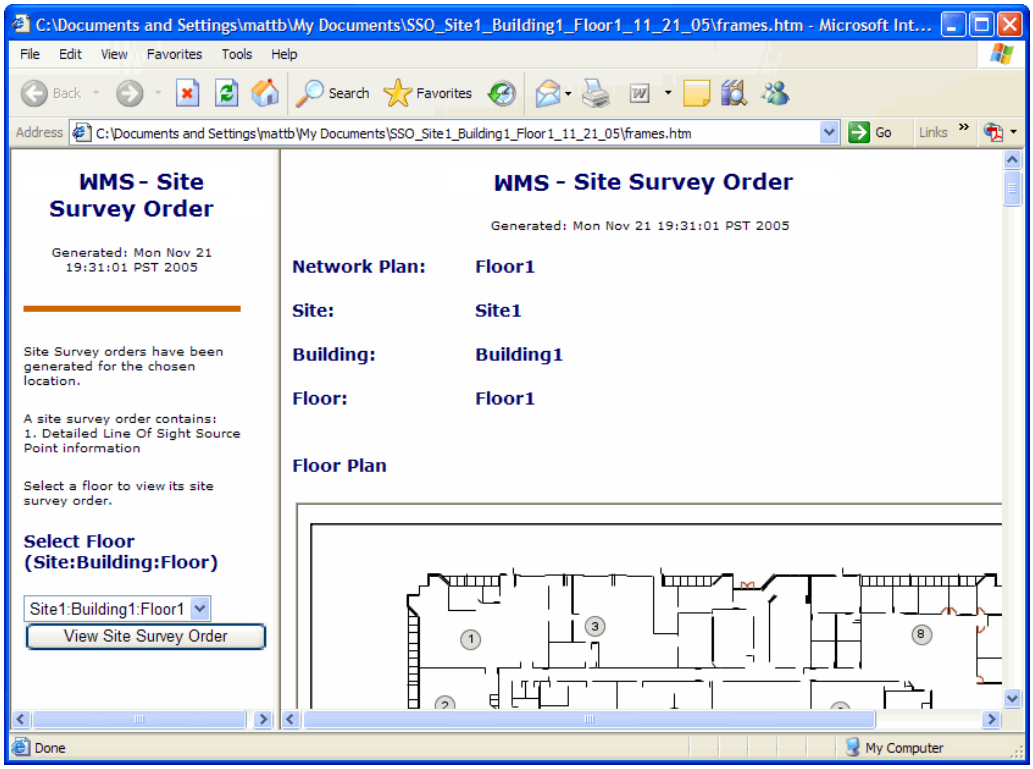
To generate a site survey order

1. Display the floor plan in the Content panel.
2. In the Task List panel, click RF Planning.
3. Under Site Survey, click Report. The Site Survey Order Generation dialog is displayed.

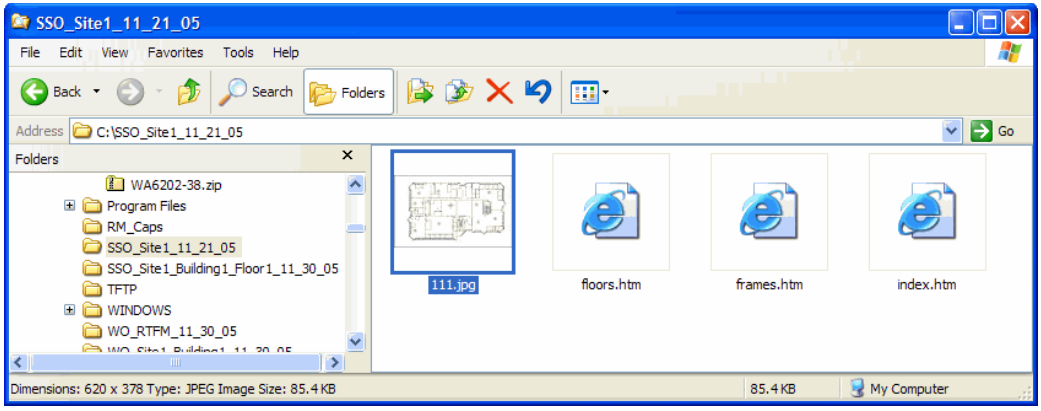
4. Select the scope for which you want to generate a site survey order. You can specify the Network Plan, an individual site, an individual building, or an individual floor.
5. Select the language: English or German.
6. To change the output directory for the report, click on the button next to output directory, navigate to the new directory, and click **Select**.
7. Click **Generate**.
8. When the report is generated, click the link in the results area to view the report in a browser window.

   A browser window containing the report opens.
9. Click **View Site Survey Order** to view the site survey work order.


C:\Documents and Settings\mattb\My Documents\SSO_Site1_Building1_Floor1_11_21_05\frames.htm - Microsoft Int...
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\mattb\My Documents\SSO_Site1_Building1_Floor1_11_21_05\frames.htm
Go Links
WMS - Site Survey Order
Generated: Mon Nov 21 19:31:01 PST 2005
Site Survey orders have been generated for the chosen location.
A site survey order contains:
1. Detailed Line Of Sight Source Point information
Select a floor to view its site survey order.
Select Floor (Site:Building:Floor)
Site1:Building1:Floor1
View Site Survey Order
WMS - Site Survey Order
Generated: Mon Nov 21 19:31:01 PST 2005
Network Plan: Floor1
Site: Site1
Building: Building1
Floor: Floor1
Floor Plan
Done
My Computer


C:\Documents and Settings\mattb\My Documents\SSO_Site1_Building1_Floor1_11_21_05\frames.htm - Microsoft Int...
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\mattb\My Documents\SSO_Site1_Building1_Floor1_11_21_05\frames.htm
Go Links
WMS - Site Survey Order
Generated: Mon Nov 21 19:31:01 PST 2005
Site Survey orders have been generated for the chosen location.
A site survey order contains:
1. Detailed Line Of Sight Source Point information
Select a floor to view its site survey order.
Select Floor (Site:Building:Floor)
Site1:Building1:Floor1
View Site Survey Order
WMS - Site Survey Order
Generated: Mon Nov 21 19:31:01 PST 2005
Network Plan: Floor1
Site: Site1
Building: Building1
Floor: Floor1
Floor Plan
Done
My Computer

10 Browse to the output directory and locate the JPEG file. Copy this file and import it into your Ekahau Site Survey tool. Proceed with your site survey.

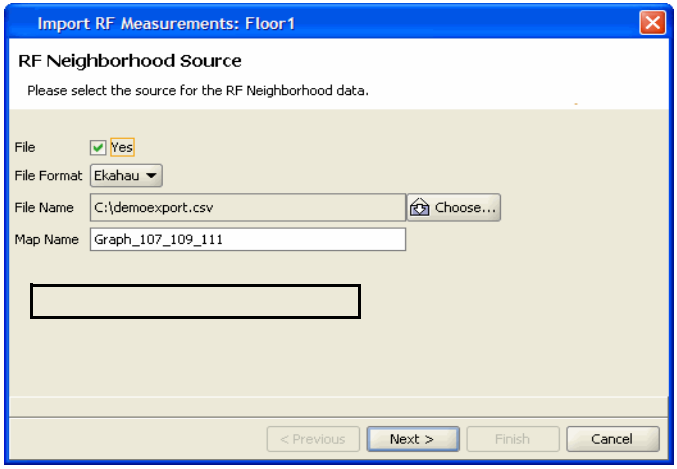


Importing RF Measurements from the Ekahau Site Survey

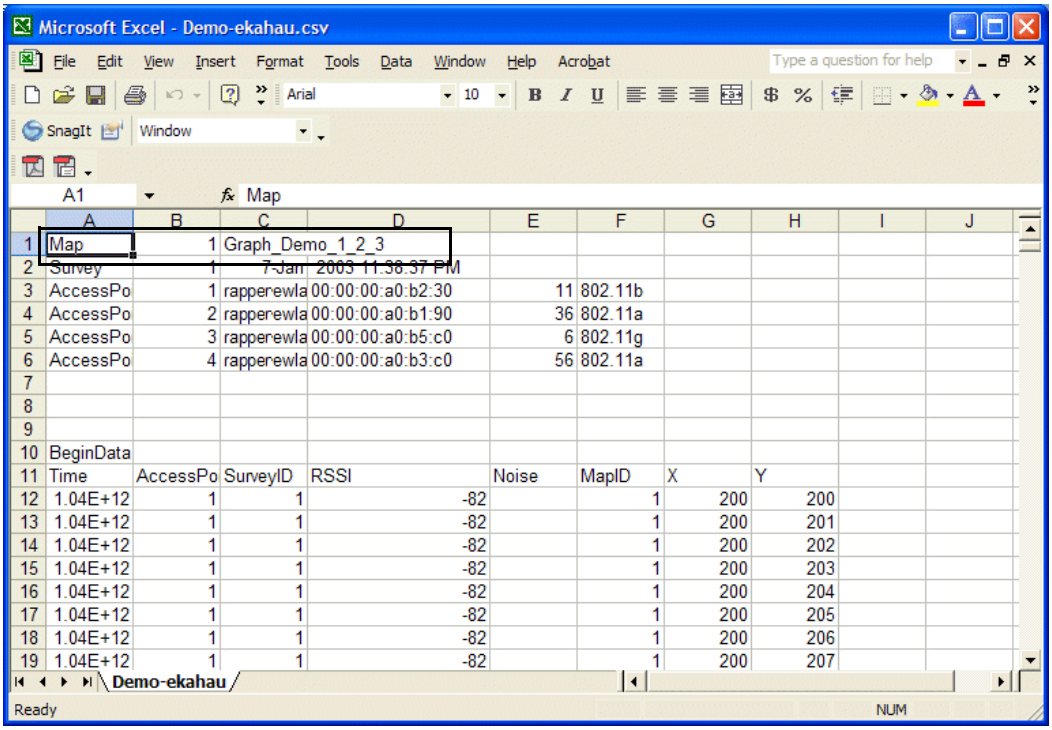
After you complete the site survey, you import the csv file containing the RF measurements from the Ekahau Site Survey tool into your network plan. After you import your RF measurements, you optimize to correct attenuation for obstacles on the floor.

To import RF measurements

1. Display the floor plan in the Content panel.
2. In the Task List panel, click RF Planning.
3. Under Site Survey, click Import Measurement. The Import RF Measurements wizard is displayed.
4. Select **File** as the source of the measurements (or, you can select both **Network** and **File**).
5. Select **Ekahau** from the **File Format** listbox.
6. Click **Choose** to navigate to the csv file that contains the RF measurement data.
7. In the Map Name field, verify the map name.



The map name in the RF Neighborhood Source window must match the map name in the top line of the .csv file from the Ekahau Site Survey tool.



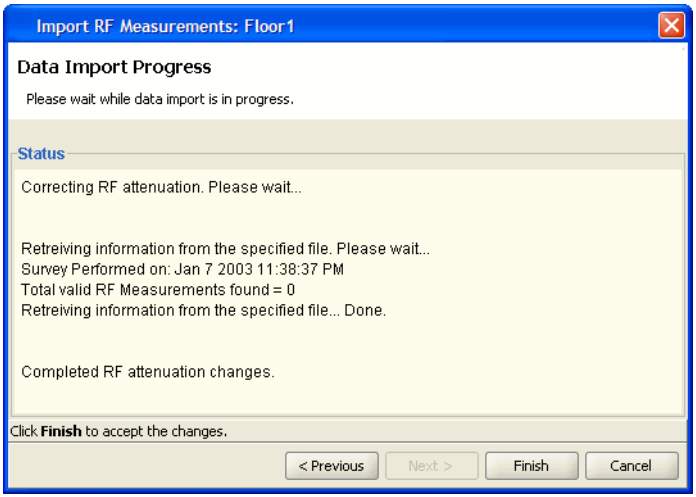
	A	B	C	D	E	F	G	H	I	J
1	Map	1	Graph_Demo_1_2_3							
2	Survey	1	7-Jan	2003 11:38:37 PM						
3	AccessPo	1	rapperewla	00:00:00:a0:b2:30	11	802.11b				
4	AccessPo	2	rapperewla	00:00:00:a0:b1:90	36	802.11a				
5	AccessPo	3	rapperewla	00:00:00:a0:b5:c0	6	802.11g				
6	AccessPo	4	rapperewla	00:00:00:a0:b3:c0	56	802.11a				
7										
8										
9										
10	BeginData									
11	Time	AccessPo	SurveyID	RSSI	Noise	MapID	X	Y		
12	1.04E+12	1	1	-82		1	200	200		
13	1.04E+12	1	1	-82		1	200	201		
14	1.04E+12	1	1	-82		1	200	202		
15	1.04E+12	1	1	-82		1	200	203		
16	1.04E+12	1	1	-82		1	200	204		
17	1.04E+12	1	1	-82		1	200	205		
18	1.04E+12	1	1	-82		1	200	206		
19	1.04E+12	1	1	-82		1	200	207		

8 Click **Next**.

The import progress is displayed. When the import is done, check the *Total valid RF measurements found* line in the progress messages.

- **If the number is greater than 0, WLAN Management Software successfully imported measurements.**

- **If the number is 0, no measurements were imported. Try the import again. If you are using a site survey file, verify that the map name is correct.**


Import RF Measurements: Floor1
Data Import Progress
Please wait while data import is in progress.
Status
Correcting RF attenuation. Please wait...
Retreiving information from the specified file. Please wait...
Survey Performed on: Jan 7 2003 11:38:37 PM
Total valid RF Measurements found = 0
Retreiving information from the specified file... Done.
Completed RF attenuation changes.
Click Finish to accept the changes.
< Previous
Next >
Finish
Cancel

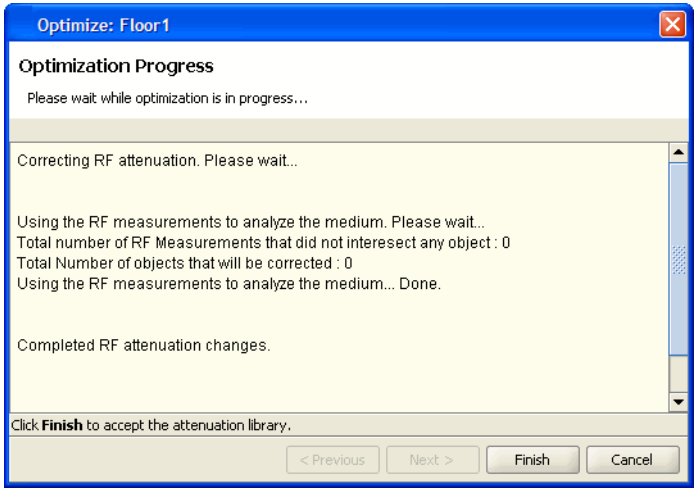
After you import your RF measurements, you correct the attenuation factors for the floor. Go to "Optimizing the RF Coverage Model" next for information about this topic.

Optimizing the RF Coverage Model

An attenuation library is a set of attenuation values for the RF obstacles on a floor. After you import RF measurements from a site survey or apply them from the RF measurements in your network to your network plan, you rebuild a floor's attenuation library using those RF measurements.

1. Display the floor plan in the Content panel.
2. In the Task List panel, click RF Planning.
3. Under Site Survey in the Task List panel, click Optimize. A wizard appears, listing the progress of the request.

Note. The RF Planning software does not support outdoor installations. RF obstacles typically found in outdoor environments have not been adequately tested for their attenuation characteristics. As a result, the database cannot ensure accurate attenuation coefficients for RF planning purposes. Nortel does not warrant or support any outdoor deployments or installations of the WLAN 2300 system implemented with the use of this tool.


Optimize: Floor1
Optimization Progress
Please wait while optimization is in progress...
Correcting RF attenuation. Please wait...
Using the RF measurements to analyze the medium. Please wait...
Total number of RF Measurements that did not interesect any object : 0
Total Number of objects that will be corrected : 0
Using the RF measurements to analyze the medium... Done.
Completed RF attenuation changes.
Click Finish to accept the attenuation library.
< Previous
Next >
Finish
Cancel

- **The *Total number of RF measurements that did not intersect any object* line lists the number of measurements that did not experience attenuation due to an RF obstacle in the path between them.**

  If the measurements came from a site survey file, they are measurements between the deployed APs and the Ekahau Site Survey tool performing the survey. If the measurements came from AP radios in the network, they are measurements between AP radios.

- **The *Total number of objects that will be corrected* line indicates the number of measurements that did experience attenuation. For existing RF objects, WLAN Management Software corrects the attenuation to match the results. If the floor plan does not have an RF obstacle where the attenuation library indicates one exists, WLAN Management Software creates an RF obstacle.**

  For RF obstacles created by WLAN Management Software, the description is **auto-generated** and the obstacle type is **Other**. You can edit these values by selecting the obstacle, clicking the Edit properties icon to open the Modify RF Obstacle wizard, and modifying the values. Click **Finish** to close the wizard and save the changes.

4 Click **Finish**.

You have optimized your RF coverage model with the new RF obstacle information. Now you can locate and fix coverage holes, or if necessary, replan your network.

Locating and Fixing Coverage Holes

After importing RF measurements and rebuilding the attenuation library, look for coverage holes by displaying coverage. Perform the following steps to locate coverage holes:

1 Display the optimized RF coverage area to view the results of the corrected attenuation data.

2 Lock down deployed APs in the coverage area (so that WMS will not move APs in your network plan during the compute and place process).

3 Compute and place APs.

4 Replan your network based on compute and place results.

Displaying the RF Coverage Area

Display the RF coverage area to view the RF coverage based on the corrected attenuation data.

To display the RF coverage area

1 Select the RF Planning option in the main WLAN Management Software tool bar.

2 Display the floor plan in the Content panel.

3 In the Task List panel, click RF Planning.

4 In the Show RF coverage using listbox, select how you want to display the coverage:

- **Baseline Association Rate—Coverage is shown based on the AP radio baseline association rate. The baseline association rate is the typical data rate the radio is expected to support for client associations. (The baseline association rate is specified during planning, on a coverage area basis.)**
- **Data Rate—Coverage is shown in colored bands that represent each of the data transmit rates supported by the radio. These rates are standard for each radio type.**
- **RSSI—Coverage is shown based on the received signal strength indication (RSSI) of the radio's signal heard by other radios.**

5 In the Coverage Areas section of the Organizer panel, select the scope for which you want to display coverage. You can display coverage for an individual radio, a specific coverage area, or all coverage areas on the floor.

- **To select multiple contiguous objects, click Shift while selecting.**
- **To select multiple noncontiguous objects, click Ctrl while selecting.**

6 On the toolbar, click the radio type (A, B, or G) for which you want to display coverage. Coverage for the selected scope(s) is displayed.

Locking Down APs

To prevent WMS from moving an AP on your network plan that you do not want to be redistributed, lock the AP down.

To lock down an AP

1 Display the RF coverage area.

For information about how to display the RF coverage area, refer to "Displaying the RF Coverage Area" on page 210.

2 Right-click on an AP in the RF coverage area, and select Lock.

Fixing a Coverage Hole

After you import RF measurements, rebuild the attenuation library, and display coverage, you can observe any wireless coverage holes in the network. To fix a coverage hole, use one of the following methods:

- Lock the APs in place, and use the Compute and Place task to recompute the number of APs needed and their recommended placement. If this results in new APs being added, install the new APs.
- Install new APs and add them to the network plan. Using this method, you install the new AP first, then integrate it into your network plan.

Computing and Placing New APs

The procedure for computing and placing new APs is the same as the procedure you use for initial planning. (Refer to "Compute and Place APs" on page 151.) Using this procedure, you can determine the number and location of additional APs you should add to your network.

Replanning Your Network

After you have computed and placed new APs in the network plan, you will need to add the APs to your network. For information about adding APs to your network, refer to either the *Nortel WLAN Access Point 2330/2330A/2330B Installation Guide* or the *Nortel WLAN Series 2332 Access Point Installation Guide*. This guide contains instructions and specifications for installing an AP and connecting it to a WSS.

After you install a new AP in the network and you want to add it to the network plan, perform the following steps:

1. Select the RF Planning tool bar option.
2. In the Content panel, display the floor plan where the AP is to be installed.
3. In the Organizer panel, click on Coverage Areas.
4. Right-click the Coverage Area to which the AP is to be associated, and select Edit Properties from the menu. The Coverage Area Properties dialog for the selected coverage area appears.
5. Click the Associations tab to display area associations information for the coverage area.
6. In the Available Access Points box, select one or more available APs to use in the coverage area, then click **Add** to move the APs to the Current Access Points box.
7. Click **OK** to close the dialog box.
8. In the Organizer panel, click on Objects to Place. A list of the APs you created is displayed in the panel.
9. Click on the AP icon, then click on the location where you installed the AP. The AP icon moves from the Objects To Place panel to its location on the floor.

What's Next?

You can create a backup copy of your updated network plan, and distribute the WMS configuration to other WSSs.

For information about administrative tasks, refer to "Perform Basic Administrative Tasks" on page 163.

Index

A

AAA security
  configuring, accounting 45
  configuring, authentication 42
  configuring, authorization 45
  configuring, overview 42
access control
  configuring 29
advisory notices, explanations of 17
APs
  assigning channel settings 154
  computing and placing 151
  locking down 210
  RF measurements from 201
attributes
  Encryption-Type 61
AutoCAD DWG files 130
Auto-RF
  configuring, initial WSS connectivity 102
  description of 37
  uploading WSS configuration 102
Auto-RF with Modelling
  adding APs 124
  adding RF obstacles 113
  adding sites 109
  associate APs 124
  creating RF coverage area 115
  description of 37

C

clean layout 138
configurations
  deploying 162
  exporting 167
  importing 167
configuring
  access control 29
  Auto-RF WSS connectivity 102
  employee access services 54
  employee access, example 56
  guess access services, example 69
  Mobility Profiles 84
  RADIUS servers 58
  rogue countermeasures 196
  service profiles 62
  VSAs 61

D

deploy
  overview of 47
  verifying 163
direct connect APs
  creating 104
distributed APs
  creating 105
distributing system images 164
distributing WSS software images 165
documentation, product 16

E

Ekahau Site Survey tool 201
  using RF measurements from 202
Ekahau Site Survey work order 203
employee access services
  configuring 54
Encryption-Type attribute 61
End-Date attribute
  description 61
event logging 49
exporting
  configurations 167

F

fixing coverage holes 210

H

hardware requirements for installation 19, 20
HP OpenView 22
HTTPS, enabling 164

I

image files
  distributing 164
image repository
  adding image 164
  deleting image 164
  using 164
importing
  floor plans 136
importing configurations 167
installation
  integrating HP OpenView 22
  license key 21
  preparing for 21
  serial number 21
  software requirements 20
  unpacking files 24
  user privileges 21
  using the wizard 24
installing 23
  equipment 158
  hardware 46
  WMS 23

L

license key 21
local changes
  deploying 162
  scheduling deployment 163

M

manage services 164
manuals, product 16
Mobility Domains
  description of 45
Mobility Profiles
  configuring 84
  creating 84
  definition 84
Mobility-Profile attribute
  description 61
monitoring
  clients 48
  displaying user activity 175
  event logging 49
  finding users 171
  group of users 179
  network status 48
  producing reports 50
  RF area 48
  rogue detection 49
  rogues 192
  verification 49
  viewing long-term user statistics 177

N

network plan 36
network plans
  saving automatically 166
  saving versions 166
network users 213
networks
  managing, overview 47
  monitoring, clients 48
  monitoring, logging 49
  monitoring, overview 47
  monitoring, reports 50
  monitoring, RF area 48
  monitoring, rogue detection 49
  monitoring, status 48
  monitoring, verification 49
  planning, Auto-RF with Modelling 37
  planning, methods to use 38
  planning, RF planning 37
Nortel WLAN 2300 System 15

O

optimal power 155
optimizing
  displaying RF coverage areas 210
  generating Ekahau Site Survey work order 203
  importing RF measurements 206
  locking down APs 210
  overview of 51
  replanning your network 211

RF coverage model 208
RF measurements, from APs 201
RF measurements, from Ekahau Site Survey 202

P

product documentation 16

R

radio profiles
applying to each radio 107
purpose of 40
RADIUS attributes
Nortel specific 61
VSAs 61
RADIUS servers
configuring 58
reporting
overview 50
types of reports 50
RF coverage areas
creating 36, 115
creating areas 144
displaying 156, 210
fixing coverage holes 210
planning 142
RF coverage model
optimizing 208
RF obstacles
adding 113
model 140
RF Planning
adding wiring closets 143
assigning channel settings 154
calculating optimal power 155
cleaning the layout 138
computing and placing APs 151
creating RF coverage areas 144
defining site information 131
definition of 129
description of 37
displaying RF coverage areas 156
generating work orders 157
importing floor plans 136
importing site surveys 142
installing equipment 158
preparing floor drawings
AutoCAD DXF files 130
RF coverage areas 142
set the scale 137
rogues
configuring countermeasures 196
monitoring 192

S

safety notices, explanations of 17
saving
network plans, automatically 166
scale, set 137
serial number 21
server hardware allocation 22
service profiles
configuring 62
configuring, Auto-RF 103
purpose of 40
services
configuring employee access example 56
configuring, guest access 69
configuring, VoWIP 85
configuring, wireless services 39
definition of concept 53
process 35
shared mode 23
site surveys
importing 142
sites
adding 109
defining 131
software requirements for installation 20
SSID attribute
description 61
standalone mode 23
Start-Date attribute
description 61
system image files
adding 164
deleting 165

image repository 164
system images
distributing 164

T

Time-Of-Day attribute
description 61

U

unpacking installation files 24
URL attribute
description 61
user privileges for installation 21
users
displaying activity 175
finding 171
monitoring groups 179
viewing long-term statistics 177

V

vendor-specific attributes. See VSAs (vendor-specific attributes)
VLAN-Name attribute
description 61
VLANs
configuring 66
VoWIP
configuring 85
VSAs (vendor-specific attributes)
configuring 61
Encryption-Type 61
End-Date 61
Mobility-Profile 61
SSID 61
Start-Date 61
supported 61
Time-Of-Day 61
URL 61
VLAN-Name 61

W

wiring closets
adding 143
creating 115
WMS
software requirements 20
WMS client 23
connecting to WMSmonitoring service 26
hardware requirements 19
installing, preparing for 21
installing, resource allocation 22
installing, standalone mode 23
software requirements 20
WMS GUI
overview 30
WMS monitoring service
configuring 26
hardware requirements 20
installing 23
installing, preparing for 21
installing, resource allocation 22
installing, shared mode 23
software requirements 20
WMSclient
installing 23
work orders
generating 157
WSS software images 165
WSSs
configuring management services 163
configuring, basic properties 46
configuring, boot information 46
configuring, connection information 46
configuring, VLANs on 66
deploying configurations 162
installing, equipment 46
uploading configuration 102

Nortel WLAN Management Software 2300 Series User Guide

Nortel WLAN—Security Switch 2300 Series

Document Number: **NN47250-101**
Document Status: **Standard**
Document Version: **02.01**
Part Code: **320665-G**
Release Date: **October 2007**

Copyright © Nortel Networks Limited 2007 All Rights Reserved
The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.
*Nortel, Nortel (Logo), the Globemark, and This is the way, This is Nortel (Design mark) are trademarks of Nortel Networks.
*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.
All other trademarks and registered trademarks are the property of their respective owners.
To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.

NORTEL